SMALL BUSINESS AND THE FEDERAL GOVERNMENT: HOW CYBER ATTACKS THREATEN BOTH

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

HEARING HELD
APRIL 20, 2016

Small Business Committee Document Number 114–057
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE
20–072 WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
RICHARD HANNA, New York
TIM HUELSKAMP, Kansas
CHRIS GIBSON, New York
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
CARLOS CURBELO, Florida
CRESENT HARDY, Nevada
NYDIA VELÁZQUEZ, New York, *Ranking Member*
YVETTE CLARK, New York
JUDY CHU, California
JANICE HAHN, California
DONALD PAYNE, JR., New Jersey
GRACE MENG, New York
BRENDA LAWRENCE, Michigan
ALMA ADAMS, North Carolina
SETH MOULTON, Massachusetts
MARK TAKAI, Hawaii

KEVIN FITZPATRICK, *Staff Director*
EMILY MURPHY, *Deputy Staff Director for Policy*
JAN OLIVER, *Chief Counsel*
MICHAEL DAY, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

SMALL BUSINESS AND THE FEDERAL GOVERNMENT: HOW CYBER ATTACKS THREATEN BOTH

WEDNESDAY, APRIL 20, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Luetkemeyer, Hanna, Gibson, Brat, Hardy, Kelly, Velázquez, Clarke, Payne, Meng, and Adams.

Chairman CHABOT. Good morning. The Committee will come to order. I want to thank you, everyone, for being here today, and we want to especially thank all of our witnesses for coming here to share your insights and expertise with this Committee on a very timely and important subject. In April of last year, this Committee heard from a panel of industry experts about how small businesses across the country are being threatened by a growing number and variety of cyber attacks. Since then, the threat to small businesses has only grown. Unfortunately, in many ways, the Federal Government's efforts to guard against this threat have not kept pace.

This morning, the Committee will look at the effects of cyberterrorism and cyber attacks on both small businesses and on the Federal Government. Small businesses face an increased risk because they lack the resources to protect themselves against sophisticated cyber attacks. We must make sure that the Federal Government is part of the solution and not adding to the problem. It is vital to both the economic and national security of this nation that the sensitive data held by Federal Government be safeguarded. The owners, employees, and customers of America's 28 million small businesses need to have confidence that their data is secure.

I think it is fair to say that confidence has been shaken in recent years with the cyber attacks on the IRS, the State Department, OPM, and even the White House. Between foreign hackers from countries like China and Russia and domestic identity thieves, the Federal Government has a target on its back that seems to get larger by the day.

This is why recent findings by the Government Accountability Office (GAO) on cybersecurity problems at agencies like the IRS and the SBA, are so troubling to me and many other members of this Committee. Just this month, the GAO reported that the IRS

paid $3.1 billion in fraudulent identity theft, or IDT, tax returns. Three billion dollars for people filing tax forms, for example, that were not the person who actually should be getting the credit back.

When the GAO testified before this Committee earlier this year, they told us that "the SBA has not conducted regular reviews of its IT investments." In these scenarios, American small businesses and consumers were put at risk due to a lack of diligence by Federal agencies. Just last week, I asked IRS Commissioner Koskinen about the data breach at his agency last May, which compromised the data of approximately 700,000 accounts. The commissioner informed our Committee that there are 1 million cyber attacks at the IRS every day. Think about that. One million cyber attacks every day at the IRS, people trying to get into files for illicit, illegal purposes.

With over 3 billion different mobile applications and $340 billion in online commercial sales last year, business transactions are moving away from the cash register and toward the smartphone. It is great to be able to order your coffee or pay your electric bill or reserve a car ride using your phone, but with this convenience comes increased exposure for both the customer and for businesses. In 2015, the average amount stolen from small business bank accounts after a cyber attack was over $32,000.

The fast pace of changes in technology means that hackers are coming up with more sophisticated methods to go after intellectual property, accounts, Social Security numbers, and anything else that can be used for financial gain or a competitive edge. With all of the uncertainty facing small businesses in today's world of e-commerce, it will take vigilance by all Federal agencies, and the watchful eye of this Committee, to ensure the data of small businesses and individual Americans remain secure. We must also look for new and innovative ways to help small businesses protect their data for this great and growing threat.

I look forward to hearing from our witnesses here this morning, and I will now yield to the Ranking Member for her opening statement.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Technological innovations are vital to our modern economy, and even more essential to the nation's small firms. In fact, small businesses are some of the savviest users of technology by using the internet to access new markets to grow and diversify. Yet, for all the benefits technology brings to the equation, it also creates additional challenges for business owners, consumers, developers, and vendors. As more consumers and businesses participate in E-commerce, protecting our financial information from cyber attacks is critical.

Unfortunately, recent data breaches at federal agencies, like the IRS and OPM, compromised financial data and personal information of millions of people. Attacks like this have made clear the weaknesses of the current cybersecurity landscape. Last year's attack on the IRS exposed over 700,000 taxpayers' accounts, and just last week we found out a former FDIC employee breached the information of 44,000 FDIC customers.

These attacks strike close to home for many of us, including small business owners. Keeping software and networks up-to-date

with the latest security is no longer enough. Cyber threats come in many forms, but they are devastating to both business owners and their customers. A single attack can wipe out a small business, which is why cybercrime poses severe problems for small businesses that are unprepared.

Sadly, some small companies fail to recognize the value of cybersecurity as an investment until it is too late. On the other hand, small firms that do recognize the importance of such an investment often lack the resources to implement an effective security system. Just as we must strengthen private sector cybersecurity, we need to ensure Federal agencies take precautions.

The testimony we will hear today will help us better protect the nation's small businesses from growing cyber threats. We will discuss the strengths and weaknesses of our federal initiatives and what more must be done for private and government data protection. In advance of the testimony, I want to thank all the witnesses for both your participation and insights to this very important topic.

With that, Mr. Chairman, I yield back.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

If Committee members have opening statements prepared, we ask that they be submitted for the record.

I would like to take just a moment to explain our timing and lighting system here. It is pretty simple. You get 5 minutes. The green light will come on there and you can talk for 4 minutes. The yellow light will come on. That will let you know you have a minute to wrap up. Then the red light will come on after a total of 5 minutes, and if you could try and stay within that, we would greatly appreciate it. The members hold ourselves to the 5-minute rule, also, and we will ask you questions then.

I would now like to introduce the panel. Our first witness is Richard Snow, owner of Maine Indoor Karting in Scarborough, Maine. Mr. Snow is here to provide his experience as a small business owner whose company was the victim of a cyber attack.

Our second witness is Kevin Dunn, technical vice president of NCC Group in Austin, Texas. He has over 14 years of experience as a professional security consultant.

And our third witness today is Nicholas Oldham, counsel at King and Spalding in Washington, D.C. In his current role, Mr. Oldham assists clients with cybersecurity and risk management, data privacy, incident response, and internal government investigations. We welcome you all here today.

I would now like to yield to the Ranking Member to introduce the final witness.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. It is my pleasure to introduce Mr. Stephen Mankowski, the national tax chair and national secretary for the National Conference of CPA Practitioners. He is also a partner at EP Caine and Associates CPA, LLC, where he advises individuals and small businesses on issues related to accounting, taxation, business consulting, and litigation support services. Welcome.

Chairman CHABOT. Thank you very much. I would now like to recognize Mr. Snow. You are recognized for 5 minutes, sir. Thank you.

STATEMENTS OF RICHARD SNOW, OWNER, MAINE INDOOR KARTING; KEVIN DUNN, TECHNICAL VICE PRESIDENT, NCC GROUP; NICHOLAS OLDHAM, COUNSEL, KING AND SPALDING LLP; STEPHEN F. MANKOWSKI, CPA, NATIONAL TAX CHAIR, NATIONAL CONFERENCE OF CPA PRACTITIONERS, NATIONAL SECRETARY, NCCPAP, PARTNER AT EP CAINE AND ASSOCIATES CPA, LLC

STATEMENT OF RICHARD SNOW

Mr. SNOW. Good morning. Thank you, Chairman Chabot, Ranking Member Velázquez, and members of the House Small Business Committee for inviting me to testify today on the current state of cybersecurity for small companies and how phishing scams have impacted my own small business.

My name is Rick Snow, and I am the owner of Maine Indoor Karting, located in Scarborough, Maine. We are an indoor entertainment venue with a go-kart track, mini golf course, arcade, and cafe. We have about 20 employees.

I am pleased to be here representing the National Small Business Association, where I currently serve as a Board of Trustee member and Chair of the Environmental and Regulatory Affairs Committee.

NSBA is the Nation's oldest small business advocacy organization with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted solely to representing the interests of small businesses which provide almost half of all private sector jobs to the economy.

Several data breaches within the Federal Government, including OPM, IRS, and DOD make it clear the government struggles to combat cyber attacks. If the government cannot protect its networks and data from cyber attacks with almost unlimited resources at its disposal, how can we expect America's small businesses to do so? Forty-two percent of NSBA members surveyed indicated that they have been the victim of cyber attack. In almost half of those attacks there was an interruption in service.

I was the victim of a phishing attack, and I have also had my credit card stolen three times. When I was phished, I received an email from my bank that there had been a suspicious attempt to gain access to my account. The email urged me to immediately log in to my account and confirm that it was, in fact, an unauthorized attempt. The link provided in the email looked identical to the log-in page of my bank. Frantic that there had been a breach, I logged in, and as soon as I typed my password, I realized what had happened. I raced to the local branch of my bank to set up a new account which took several hours. It took about a week to get the new checks and debit cards for the new account to us. Since we used the cards and checks for all our bills and local purchases for our business, I had to either use our company line of credit or my own credit cards. This is not unusual as many small business own-

ers often need to use their personal credit cards to support their business, especially during difficult times.

The financial cost to my business paled in comparison to the delays and disruptions. My wife, who runs the day-to-day operations of our business, and her work were limited because she spent the week trying to update all of the vendors with the new account information.

According to the NSBA 2015 Year-End Economic Report, in 10 percent of cyber attacks, a bank account was improperly assessed. I was one of those. Two weeks after the initial phishing attack, I logged into our new account late Friday evening, and to my horror, found that my balance was zero. It was payday and I was terrified that the paychecks that were issued that day would not clear. We are supporting a number of families, many of which live paycheck to paycheck and could not have made it without that particular payday. I quickly discovered that three wire transfers were made that night to three different bank accounts around the country totaling $15,000.

This is an ongoing threat of internet age, and it will evolve as long as the internet continues to facilitate commerce in the global economy. It is unlikely that there will be one solution.

I am sorry. I missed a page. So, excuse me. Sorry.

After a night of no sleep, I had to be at the bank first thing Saturday morning. I was lucky and was able to stop the wire transfers. I had to then spend another day away from work opening another account and going through the process of getting all my new cards and ordering new checks. My poor wife had to spend another week updating vendors. She spent the better part of 2 weeks away from her normal duties because of this phishing incident.

My bank told me that this was a standard phishing loss and that I was lucky that I discovered it before the 48 hours had lapsed so no money was actually stolen. My business accounts were not protected against theft the way that my personal accounts would be, so the losses would have been on my business. This attack could have ended my business if I had not been able to recover the money. Most small businesses do not have a significant cushion to absorb these type of losses, and we are no different. Losing thousands of dollars during a tough time in the economy can make a significant different for me, my business, and my employees.

As small businesses become increasingly dependent on the internet, they become a larger target for cybercriminals. These threats are very real and immediate. In fact, 94 percent of small business owners indicate they are concerned about being targeted by cyber attacks. For many small businesses, a cybersecurity incident could lead to an entire network being down for many days until the full extent of the problem is known and then fixed.

This is an ongoing threat of the internet age and it will evolve as long as the internet continues to facilitate commerce at the global economy. It is unlikely that there will be one solution to stop the attacks. In fact, slowing and preventing these attacks will most likely require an ongoing process to identify new threats, vulnerabilities, and ultimately, solutions. I urge Congress and this Committee to always bear in mind the unique challenges that

small businesses face and continue to include the small business community in that process.

Thank you for allowing me to testify before the Committee today, and I would be happy to answer any questions that you might have for me.

Chairman CHABOT. Thank you, Mr. Snow, for your testimony today. What a scary situation. Thank you.

Mr. Dunn, you are recognized for 5 minutes.

STATEMENT OF KEVIN DUNN

Mr. DUNN. Good morning, Mr. Chairman, Ranking Member Velázquez, and other esteemed members of the Committee. Thank you for the opportunity to testify today.

My name is Kevin Dunn, Technical Vice President for NCC Group. For the last 15 years, I have dedicated my career to carrying out cybersecurity attacks against private companies and government organizations. I am not a criminal; I am a penetration tester. For our actions in this highly specialized field, my colleagues and I determine ways to break into organizations via cyber and physical means. Specifically, we are hired to identify vulnerabilities that allow a company's security to be compromised. This exercise subsequently allows us to provide customized advice to our clients, detailing the short- and long-term actions they should take to reduce their susceptibility to attack.

My testimony today will focus on four areas: the strengths and weaknesses of cybersecurity training, increasing security when using cloud service providers, the potential impact of small business security on the government, and the benefits of a data-driven risk model.

To evaluate the state of high level cybersecurity training designed for small businesses, I would like to explore two examples: training provided by the U.S. Small Business Administration and training provided by the Federal Communications Commission. Through these trainings, small businesses are able to gain awareness of important cybersecurity threats such as the dangers associated with phishing emails, malicious websites, malware, ransomware, and the typical motivations of attackers. This information provides an ample start for educating small businesses in a general awareness capacity and extends to providing cybersecurity tips for the major areas of concern. However, the training and guidelines are high level in nature and lack the depth of information needed to convert directly into hands-on actions. In the world of small business IT support where efforts are typically coordinated by owner-operators, this information may not be comprehensive enough to make a worthwhile difference beyond providing general education.

Many small businesses use cloud service providers to implement important services like email, file storage, and data backup. This often unburdens the IT administration overhead from small business owner-operators or small businesses with a one- or two-person IT team. The use of third-party cloud service providers is typically a positive security move for small businesses. The attention to security from the major providers in this space affords a number of

features that greatly increase the security of data for a small business.

However, it should be noted that there are additional features that should be enabled to make attacks harder for adversaries. These features are often not enabled by default. Chief among these is the use of multifactor authentication. The majority of major online services now support the use of multifactor authentication using at least SMS messages to a cell phone as a means of out-of-band authentication. But despite this inexpensive option, it is often overlooked by organizations that use cloud services or internet services, relying instead on single factor authentication in the form of user names and passwords.

The impact of a small business on the government should be considered in at least two key ways. The first concerns the direct and indirect connectivity between a small business and a government network. The second concerns small businesses in the government supply chain. A small business with a direct connection to a government network is likely a rare occurrence, but in such a scenario, if the small business is compromised sufficiently, an attacker's ability to traverse to a government network could be a simple task. However, examples of indirect connectivity are more common and are typically databased in nature. When government users consume the services of a small business, their user names, passwords, personal information, and other data could be used in a subsequent attack against government systems if extracted from a compromised small business system. Of course, the reverse is true as well.

The second area to consider is when a small business is in some way part of the supply chain to a government department or agency. The most typical examples of this are where a small business develops software or hardware that is subsequently installed on government networks.

Finally, a good way to think about security and a means to ensure that the approaches chosen to secure your organization are fit for purpose is to think first about the data you care about. Considering the data first is an excellent approach and one that is advised in the FCC's small business cyber plan at all. However, too few organizations actually consider their data or subsequently plan security around the value of different data types. Even fewer organizations consider what will happen when, not if, an attacker gains access to their data. Using a data-centric risk management model would allow small businesses to focus their security attention where they need it most.

Thank you again for this opportunity to address this Committee. I will be happy to answer any questions.

Chairman CHABOT. Thank you very much.

Mr. Oldham, you are recognized for 5 minutes.

STATEMENT OF NICHOLAS OLDHAM

Mr. OLDHAM. Mr. Chairman, Ranking Member, and members of this Committee, thank you for allowing me the opportunity to appear before you today.

I have been involved in cyber issues for many years as a former Federal prosecutor at the U.S. Department of Justice, and now as

an attorney at King and Spalding. In my practice, I counsel clients, both large and small, on cybersecurity risk management. Our interconnectivity is growing at an astonishing rate. This interconnectivity, especially the internet of things, holds tremendous promise for consumers and companies. It also creates new challenges in terms of cybersecurity because anything connected to the internet can be hacked.

Cyber attacks cost businesses billions of dollars every year as a result. Where do small businesses fit into this landscape? The interconnected world lets small businesses develop new products and services and compete across the globe, but with cybersecurity, small businesses often get burned at both ends. They are less likely to have the resources to prevent breaches, and also may have fewer resources to respond to those breaches. It can be difficult for small businesses to find the right information and training, and the cost of mitigation measures in response can significantly impact a small business' bottom line.

As a lawyer, I do not manage corporate networks. I do not conduct vulnerability testing. Rather, I believe that cybersecurity is as much a people and a process issue as it is a technical issue. I focus on the people and process side of the equation, addressing the legal and business cybersecurity risks faced by companies. I also help manage companies comply with their legal obligations, interact with various regulators, and respond to regulatory enforcement actions and litigation. These legal and business costs, including compliance costs, drain on employee morale, and time and reputational damage can be significant.

There are at least three ways the government can play a role in lowering these costs. First, by addressing the cybersecurity education gap. When weighing the costs and benefits of enhancing their cybersecurity, companies may find that it is far more expensive to not implement basic security measures. The problem here is that there is a cybersecurity education gap. Small businesses may not find the information they need to properly assess and mitigate these costs.

Bridging this education gap can be difficult for small businesses, especially those that lack the resources to hire specialized employees or cybersecurity experts. Even when information is available online, it is often difficult to find, rarely updated, and often inadequate.

In many ways, cyber threats have analogs to traditional crime. In the traditional crime scenarios, small businesses would likely call the local police department for best practices in preventing or responding to crime. In the digital crime scenarios, there is no one logical place to call. The government may have a role in bridging the cybersecurity education gap by encouraging the development of cybersecurity education resources and connecting them to those who need them in the private sector.

Second, many of the cybersecurity initiatives receiving the most attention are not necessarily tailored to small businesses. For example, the NIST cybersecurity framework is emerging as a leader, which is a promising development. This could simplify the landscape for small and large businesses alike. The current iteration of the NIST framework, however, is not particularly geared towards

small businesses. It can be difficult and expensive to understand and implement regardless of business size, and until it is better tailored to small businesses, for some of them it may just be one more program that they cannot afford to keep up with.

Perhaps more importantly, a small business might become subject to a cybersecurity framework by virtue of its contractual relationships. In this case, the small business might inadvertently expose itself to significant liabilities and cyber risks. While good cyber hygiene is important, to improve the NIST framework and similar programs and policies, the government should make a serious effort to increase the involvement of small business owners in all phases of the legislative and rulemaking process.

Third, the current regulatory regime for cybersecurity presents additional difficulties for small businesses who will inevitably struggle to determine both what cybersecurity measures they are required to meet, and when a breach or attack does occur, what procedures the law requires them to follow. There are currently 51 different State or territory data breach notification laws and many of them are inconsistent with each other. I have seen a growing number of Federal agencies also stepping into this space.

In short, there is a need to clarify and simplify what companies must do. Because of the complicated and evolving landscape, the on-the-ground expertise of the private sector must necessarily play an important role in these efforts.

Thank you for the opportunity to testify today, and I look forward to your questions.

Chairman CHABOT. Thank you very much.

Mr. Mankowski, you are recognized for 5 minutes.

STATEMENT OF STEPHEN F. MANKOWSKI

Mr. MANKOWSKI. Thank you. Mr. Chairman, Ranking Member Velázquez, and members of the Committee, thank you for inviting me to testify today.

My name is Stephen Mankowski, a partner with EP Caine and Associates, the Executive Vice President of NCCPAP, the National Conference of CPA Practitioners, and a member of the AICPA.

NCCPAP has been at the forefront of identity theft issues through our advocacy and testimony at prior hearings dealing with ID theft. NCCPAP members have helped guide numerous clients who have been victims of identity theft.

ID theft has been growing exponentially for years. It seems that no matter what controls are put in place, criminals have better and more focused resources to circumvent these safeguards.

The IRS reminds practitioners that they must be vigilant with their system integrity. Criminals are aware that the prize for breaching tax practitioner systems could yield not only names and Social Security numbers, but also several years of earnings, as well as bank information and dates of birth. Two Midwestern firms were compromised this tax season and had fraudulent returns submitted by utilizing their Electronic Filing Identification Number or EFIN.

While firms are required to obtain an EFIN from the IRS to electronically file tax returns, paid preparers are required to use a Practitioner Tax Identification Number or PTIN. Firm information,

including their Employer Identification Number, however, still appears on their tax return. Given the risk of firm ID theft, why has the IRS not adopted a firm PTIN, something that NCCPAP strongly recommends.

Over the past year, as noted by the other panelists, the IRS has had multiple system breaches. First, the IRS online transcript program, Get Transcript, was compromised in May 2015. The number of accounts affected now exceeds 700,000. The second breach was related to the IP PIN retrieval tool that was contained on the IRS website and is more troubling. The taxpayers who have IP PINs have already been victims of tax refund fraud and obtained the six-digit IP PIN to prevent further unauthorized account access or tax filings. This tool had been used using the same interface as Get Transcript but had remained available to the public, and unfortunately, those less scrupulous.

Social Security uses a banking prenote to verify the accuracy of the recipient's banking information prior to the initial payment. Unfortunately, the IRS refund system does not include prenote account verification. The implementation of a prenote system could result in a significant reduction of the annual $3.1 billion misappropriation of government funds.

While it is easy to understand that taxpayers want to receive their refunds as quickly as possible, one must ask a simple question: Is paying a tax refund in 7 to 10 days prudent? A recent survey by Princeton Research Group noted that 22 percent of taxpayers surveyed would be willing to wait up to 6 to 8 weeks to receive their refund if they knew it would combat identity theft.

Taxpayers are urged to protect their personal data, but with widespread internet usage, online shopping, and criminals just waiting to pounce on unsuspecting victims, ID theft continues to grow. Individuals and businesses remain the target of cyber attacks and must remain cautious when opening emails with attachments, visiting web pages, or simply paying for the family groceries. Taxpayers often do not realize they have been a victim of tax-related ID theft until their electronically filed tax return gets rejected. Once a taxpayer has been victimized, they expect to obtain an IP PIN from the IRS, and starting in January 2017, they automatically will.

In conclusion, NCCPAP feels that using the prenote technology that already exists and is used throughout the financial industry would allow taxpayers to continue receiving their refunds promptly while reducing refund fraud.

Further, NCCPAP urges Congress to pass legislation to provide the IRS the necessary authority to regulate all tax preparers and require paid preparers to meet minimum standards. Currently, only CPAs, EAs, and attorneys are subject to the requirements of IRC Circular 230.

Finally, NCCPAP calls on Congress to provide the necessary funding for the IRS to continually modernize and upgrade their systems to minimize and eliminate data security breaches. The first step would be Congress reauthorizing streamline critical pay authority to allow the IRS to secure top IT talent without a 3- to 6-month waiting period.

Thank you for the opportunity to present this testimony, and I welcome your questions.

Chairman CHABOT. Thank you very much, and we appreciate the testimony of all the witnesses here this morning. It was excellent.

Mr. Snow, first, let me apologize to you for having to return a call there before your testimony. I apologize for that, but I had your written statement ahead of time, so I am prepared.

You experienced a worst-case scenario for a small business cyber theft. What advice would you give to others who are put in the same or a similar situation?

Mr. SNOW. The first thing I would do is to ensure that when you look at the website at the top, web ID, that there is a https ID, and that would have prevented that from happening. I just learned that in that process. But it would be very difficult to stop someone from just accessing the way it was with me because it was an identical website to the bank website. The login looked identical. In fact, there was no difference.

What was more disconcerting to me was the fact that they stole the new account number, and to this day, no one understands how that happened; how they were able to access a brand new account opened with all that information and move money out of the new account, not the old account.

Chairman CHABOT. How long did it take you to straighten all this out?

Mr. SNOW. The whole process was about a month because, the first time we had to rush everything because they have to print new checks and new credit cards and everything, so it was about a week and a half. Then when we discovered the loss, it was 2 weeks later. Then we had another week and a half or so of additional time to go through that whole process again.

Chairman CHABOT. Mr. Dunn, in your testimony, you provided the example of using text message authentication as an inexpensive use of multifactor authentication. Are there other inexpensive steps the Federal Government or small businesses could make in order to verify accounts?

Mr. DUNN. Yes. I think that you can use email. There are a number of channels that you can use. The situation really is that when you rely on just one thing, in perhaps this case as well, just a username and password, that that is a single point of failure. The point is to have more than one authenticating factor. A number of things could do that so long as it is out of band from the process.

Chairman CHABOT. Thank you very much.

Mr. Oldham, protecting the privacy and civil liberties of Americans is obviously an important component of cybersecurity discussions. What effort is the private sector making to protect consumers in this area?

Mr. OLDHAM. One of the key goals is transparency, communicating to consumers what information is being collected and how is it being used. That has become even more important as the ecosystem is growing so that everything is connected, multiple third parties and the like, and the third party would include, for instance, sharing information with the government. I think the most

critical step the private sector is taking is ensuring that there is this transparency.

Chairman CHABOT. Thank you very much.

Mr. Mankowski, in your testimony, you gave a firsthand account of how a tax preparer dealt with confusion and delays with the IRS in response to a data breach. What would you recommend to the IRS for future responses to a tax preparer once a breach has been confirmed?

Mr. MANKOWSKI. That is a very good question, Mr. Chairman. What I would recommend, first of all, is that I have reached out to my contacts that I deal with through some of my committees at the IRS, and it is being addressed tomorrow at a monthly meeting. But in addition, I would advise practitioners to know who their local stakeholder liaisons are so they have an area that they could reach out to so that they can start the process of communicating with the IRS when they suspect there may be a breach, not once they actually confirm. Because during that period of time, if their EFIN was being used improperly, the IRS could have stepped in very quickly, disabled their EFIN, and could have potentially stopped fraudulent returns from being processed.

Chairman CHABOT. Thank you. Let me give you another question. You mentioned a recent audit where 6 of 13 e-filing sites failed to take steps to protect consumers from fraudulent and malicious emails. What recommendations would you offer these sites in order to improve their cybersecurity?

Mr. MANKOWSKI. That is also a very interesting question. I believe that is one that Mr. Dunn could probably help with as far as the cybersecurity aspect. But they would certainly need to ensure that as they are going through their systems that they are making sure that any incoming emails are being checked. There has been widespread spoofing of calls as well as emails coming in to companies that are purporting themselves to be high-level individuals within a company asking for data that they would normally be asking for, such as W-2s and such, that everything looks to be coming from that individual, everything looks the same, just the email address may be slightly or just something a little bit off. Companies really need to be vigilant as to looking at who emails are coming in from, and if they are not sure if it is legitimate or not, they should pick up the phone and call the person who they are actually getting this request from. Simply responding to that email, you are responding back to the criminal. Of course, they are going to say, oh, yeah, I am so-and-so, and I need to get this information to finalize a report for the board. They are further spoofing. They just need to be careful when they are responding, and as Mr. Snow had mentioned, making sure that any websites they go into do have the https that would mean that it is a secured website.

Chairman CHABOT. Thank you very much.

Mr. Dunn, I would follow Mr. Mankowski's advice, except that I am out of time, and I like to hold myself to the same rules I do everybody else. So I will yield back my time, and the gentlelady, the Ranking Member is recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Mr. Mankowski, last week we had the Commissioner of the IRS here testify before our committee, and he talked about the

Cybersecurity Summit between the IRS and tax practitioners. From the industry perspective, do you believe this partnership is effective at preventing tax fraud?

Mr. MANKOWSKI. I think it is a very good first step, and they have already shown that it has been successful. They have met with, and they have included initially people from State associations, State government, as well as the banking and software community, to work on trying to prevent tax returns at the onset when they are being processed into the IRS system. They have gone further and expanded their focus now to starting including practitioners into their groups, and they are estimating that last year, with the first year of their summit, they prevented in excess of 3 million fraudulent returns from getting into the system. Now they just need to understand that returns are, unfortunately, getting through the filters, so now they need to keep working on filters during the processing and primarily protecting the refunds because that is taxpayer dollars, as well as government funds, that are being misappropriated.

Ms. VELÁZQUEZ. Thank you.

Mr. Snow, I am concerned that typically, small business owners view an investment as a way to increase revenues, yet, with cybersecurity they are expected to make an investment in order to prevent revenue losses. So is it often hard to persuade small firms to spend money without seeing an immediate return? What needs to be done to bridge this gap?

Mr. SNOW. I think the number one issue that we have as a small business is that every single thing leads to the bottom line. Every decision you make adds a cost. In our case we have added insurance, cybersecurity insurance, to our overall cost. The unfortunate part of that is that the deductible is very high. It is a $5,000 deductible. For me, I am out that immediately. That is the same as my burglary insurance as well. When we have someone break into our building, which happened a few months ago and they destroyed our security system, it cost us $5,000, which is also our deductible. We are out that money. That happened to be all the revenues that we had for that particular month. So it really eats into our bottom line. It is very expensive.

Ms. VELÁZQUEZ. Mr. Dunn, in your estimation, how much would it cost a company, a small company, one with fewer than 250 employees, to become cyber safe?

Mr. DUNN. I think it is very hard to provide that estimation because it really depends on the data that they hold, the types of inputs and communication channels they have. We could be talking about a very simple setup or we could be talking about a very complicated setup. It is true that the cybersecurity industry has a certain price point that currently is very difficult for small business owners to take part in. Certainly, we are probably talking thousands of dollars in order to get consultative help.

Ms. VELÁZQUEZ. Thank you.

Mr. Oldham, who do you think is best situated to handle cybersecurity threats, the federal government or private industry? Or do you think some sort of balanced public-private partnership is needed to properly address cybersecurity needs?

Mr. OLDHAM. I think the balanced public-private partnership is the key. This industry is evolving so rapidly, and when the government gets involved, it becomes very static. I think it is important to make sure the private sector has a huge input, and that is why I think something like in this framework is a great start because it is voluntary. It attempts to coalesce the best standards that are out there, but it is also something that has a recognition that it needs to evolve over time. My worry is tipping the scale to one side or the other will cause the current industry to stagnate more.

Ms. VELAZQUEZ. What type of recommendations would you offer for encouraging that type of partnership?

Mr. OLDHAM. Number one, supporting NIST's efforts and what they are doing. Right now, NIST has put out a framework. It has had some widespread success but also quite a bit of criticism from industry. They held a workshop last month where they heard from several sectors of the industry, including small business, that it is not really approachable and useful. Just as a big picture, the NIST framework was designed for critical infrastructure, so it is not approachable for small businesses, ensuring that the NIST is putting the appropriate emphasis on adapting itself to particular market sizes and industries.

Chairman CHABOT. The gentlelady's time has expired.

Ms. VELAZQUEZ. Thank you.

Chairman CHABOT. Thank you.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Chairman CHABOT. The gentleman from New York, Mr. Gibson, is recognized for 5 minutes.

Mr. GIBSON. Thanks, Mr. Chairman. I appreciate the opportunity here today to hear from the panelists' illuminating testimony provided.

Mr. Snow, I want to begin with you, just a point of clarification. You, in telling us about what had happened to you, you had made the comment that, fortunately, within 48 hours you were able to take action. What was implied in your statement is we have a differentiation between business and personal liability or accounts. I am looking for clarification. Is there some dimension of FDIC that protects people? Why is it different? If you could just help me understand that, number one.

Mr. SNOW. Number one, I do not know the exact ramifications. My understanding was because it was a wire transfer there is a 48-hour time that it runs. If you can stop it within that timeframe, the money does not actually transfer or they can call it back, the bank, with the interbank processes.

Mr. GIBSON. Do any other panelists know the answer for that? Why is it that business does not seem to have the same protection as an individual? One of my constituents out there, if somebody was to do a phishing expedition on them and they would be under similar circumstances, I am curious if anybody knows the answer to that.

Okay, for the Committee, I think that is something probably worth checking into. A concerning situation. I am glad it worked out okay for you there.

Then Mr. Oldham—even though I know that it was Mr. Snow—it was very burdensome and onerous on your bottom line based on

you had to divert resources. Mr. Oldham, in one of your comments you talked about that the Federal Government might want to look at clarification or clarity in terms of what companies must do when these circumstances happen, reporting requirements and the like. What is your understanding of what the SBA requires now with regard to—or the United States Government—in terms of a protocol when a company faces an attack?

Mr. OLDHAM. I am not aware of anything from the SBA, but the notification requirement at large are a hodge-podge. If it involves financial information, the Gramm-Leach-Bliley Act would require notification. If it is healthcare information, regulations under HIPAA would require notification. Each of the State data breach laws have different definitions, and I think one of the key concerns, especially if you are a small business and you may have information involving people from multiple jurisdictions or multiple types of information, there is an enormous cost of just figuring out what you have to do at the beginning.

Mr. GIBSON. I appreciate that comment. In fact, it mirrors some of my experiences in the U.S. military. I think that is also worthwhile for the Committee to capture that. Maybe we should consider a clearinghouse requirement that really socializes, if you will, what companies must do under these circumstances.

Finally, for the panel, I would love to hear your insights on this question, that with regard to science and technology, research and development, sort of blue sky, if you will, what do you think, based on your experiences, would be a worthwhile endeavor to address the issue of cyber attack at large—on businesses, on people, on government—on where you think we should put emphasis on for science and technology, research and development, to protect?

Mr. DUNN. I think in most cases, every incident I have ever been involved with, the visibility of what is actually happening from a data and packet level is never where it needs to be. I would definitely like to see strides in that direction, some way of increasing the ability for us to understand from a network and data perspective what has happened in a given scenario.

Mr. GIBSON. Thank you.

Mr. SNOW. I think the most frustrating thing for me was to realize that someone at the receiving end of that money was going to show up and get that money, and that there was no action taken. On my private credit card thefts, purchases were actually made. The merchant was out of that merchandise. Obviously, they got the money for that merchandise, but we absorb it as all of the consumers in the overall doing business. There is no authority trying to stop these people, that I know of, trying not catch these people who are making these purchases with fraudulent credit cards or other things. That is the frustration that I have. I know that I can call my local police when they break into my building. If I walk into a bank and demand money, the FBI will be chasing me forever. But in this case, there is really no action that is done beyond what we had to do as individual business owners.

Mr. GIBSON. Thank you. Mr. Chairman, I see my time has expired. I wonder if maybe science and technology, research and development into biometrics, is a possibility as a surety for any kind

of transaction is worth our endeavors. But I thank the Chairman for the opportunity.

Chairman CHABOT. Thank you very much. The gentleman's time is expired.

The gentlewoman from North Carolina, Ms. Adams, who is the Ranking Member of the Investigations, Oversight, and Regulations Subcommittee is recognized for 5 minutes.

Ms. ADAMS. Thank you, Mr. Chair. Thank you, Ranking Member Velázquez, for hosting this hearing.

Some of you have mentioned the importance of education and training in cybersecurity. I am long-time educator and very interested in what we can do there.

The Federal Government is involved in this in a number of ways. For example, last year, the Obama Administration announced the New Cybersecurity Consortium consisting of 13 Historically Black Colleges and Universities, HBCUs, two national labs, and a K-12 school district. The goal is to create a sustainable pipeline of students focused on cybersecurity. My question to any of you, is the Federal Government doing enough to provide the kinds of expertise that small businesses need to ensure their cybersecurity? If you could speak to maybe some relationships between educating students beyond this point.

Mr. MANKOWSKI. Ms. Adams, I will start the discussion. I believe that from a tax standpoint, the amount of education really starts from the government, from the IRS. As practitioners, we are continually discussing this with our clients that the IRS, with the different phishing phone calls and the email scams, that the IRS currently is not phone calling or emailing people. If they get any of these calls, they should hang up. If they get a email that says it is from the IRS, that they have an extra refund, just delete it, because they are not going to be authentic. But every day during tax season, it seemed my office was getting a phone call from someone who received a phone call that they were getting ready to get arrested. My partner in my firm had gotten a similar phone call. We actually had a little bit of fun with the people. We kind of strung them along for a little bit. But as times are changing, with the rules that were passed recently with collections within the IRS, some of that, as the collections get outsourced, the companies that are going to be taking over will be calling and could potentially be emailing our clients. It is going to create an even greater disparity of the education because what we have been telling our clients for years, come whatever point that the IRS is able to implement that process, everything we have worked on and gained with our clients over the last few years will pretty much be thrown out if they start getting phone calls from a collection for old tax balances. Thank you.

Ms. ADAMS. Mr. Oldham?

Mr. OLDHAM. I think there are two separate issues; both are very important. One is educating students as they come up about cybersecurity. That is critical. Just like educating people how to balance their checkbook to keep good financial sense, teaching people good cyber hygiene is going to be imperative for minimizing the cyber threats in the future.

Today, educating small businesses can be more challenging because they have not had the years of education, such as a secondary student. However, the biggest issue that I see is that there is not a lot of helpful information out there that is practical and granular for small businesses. In fact, in preparation for my testimony today, I searched around the internet looking for small business guides and was surprised that in many locations, including on government websites, the links were broken, the guides were out of date, or the guides were so high level that I do not know how an owner-operator without IT security background would be able to implement security measures based on those guides.

Ms. ADAMS. Okay. Well, let me move on to another question. Online marketplaces, such as eBay, have given small businesses greater access to suppliers and customers abroad. A McKinsey Global Institute study found that 97 percent of U.S. small- to medium-size businesses on eBay engage on export to other countries. My question is, do these marketplaces and international transactions expose small businesses to greater cybersecurity risk?

Mr. Dunn, if you want to answer that?

Mr. DUNN. I think the websites themselves and the online marketplaces do have to be vetted, do have to be verified to understand if they have any security flaws because, having a security flaw in a marketplace like that will expose the vendor and the small business to potential attacks. Understanding if there are any flaws in that marketplace is really critical.

Ms. ADAMS. Quickly, Mr. Dunn, you talked about the use of cloud computing. What is the best way that small businesses could benefit from using cloud providers to improve their security?

Mr. DUNN. I think not doing conventional IT in-house is a good move. Using email and file storage from a cloud service provider will be beneficial because it is not on premises, and typically, the major providers of those services are doing a lot in security and more than a small business could do.

Ms. ADAMS. Thank you. I am out of time, Mr. Chair. I yield back.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

The gentleman from Mississippi, Mr. Kelly, is recognized for 5 minutes.

Mr. KELLY. Thank you, Mr. Chairman. I thank each of you witnesses for your insight here today.

First of all, I would like to echo what the gentleman from New York, Mr. Gibson said. I think it is important for us as a Committee to find out if there are different rules for persons and small businesses and then large corporations to make sure that we are protecting each of those in an appropriate manner.

Second, Mr. Snow, it is a travesty what happened to you, but that story is repeated over and over again across this nation. As a former district attorney, I can tell you that there is a lot of room that we can improve in this. Do you have any specific areas that you think the Small Business Committee or the Small Business Administration can help to either educate or inform the general public and small business users that we can take forward?

Mr. SNOW. Thank you. I believe that education is probably the key. Obviously, cost is another big concern for every small business. When you start a business, capital is usually at a premium, and when you sit down, in my case, I have close to 70,000 members who come in and race at my track throughout the time that we have been open. I have their data, and it is in a server that I have to protect. That is a concern. My software is provided by a Belgium-based software company, so I have to have access to them. They come in at night to update and upgrade the system on a regular basis. In an international marketplace that we are in, I think education is very important so that the small businesses understand. The other issue is the liability is significant, and a lot of small businesses do not understand that. When I sat down with my insurance agent to renew our insurance, that was one of the questions I asked, and I was amazed, number one, at the cost to get the coverage, but number two, how few businesses actually apply and get that coverage. It can be very expensive for a small business.

Mr. KELLY. Mr. Oldham, going back, as I said, first of all, thank you for your service as a prosecutor. I think they are some of the most important people enforcing this law, and being a former one, I am obviously biased in that. But I thank you for your service. As a former district attorney, I was on the local level or I was on the State level, and you as a Federal prosecutor. Quite commonly what I saw is that, number one, when small businesses or individuals are victimized, they do not know who, how, what they need to report.

The second thing that I saw is quite often the jurisdictions are not clear. It is not clear where it is coming from, and they do not inform other jurisdictions, so they do not know if it is Federal, they do not know if it is State, they do not know if it is county, they do not know if it is the next State over. It is outside the jurisdiction of this hearing, but I think it is important that we inform law enforcement on how to deal with this and small businesses on how to inform law enforcement so there is a database that we can use to stop this. Do you have any ideas in that area?

Mr. OLDHAM. I would say generally the jurisdiction issue is a major issue in prosecuting cyber crime cases. The resources are not there at the local level and it is hard to chase criminal information that is as wide as the web and tracks lead everywhere in the world.

I think, going back to the education point from earlier, training local enforcement who are going to get the calls from businesses that have been breached on who to report to, who is the right person in the Federal Government who can help, or where is this database, as you mentioned, would be incredibly helpful to make sure the information is not just coming in for prosecution, but also going out to help the small businesses around the country.

Mr. KELLY. On that same line, quite often, these people who take advantage of small businesses or individuals move from jurisdiction to jurisdiction, and there is not any database that gets us ahead of the curve. Quite commonly, they use the same scheme. From Mississippi, they will move to Alabama, they will move to Tennessee, they will move to New York City, but they continue to do that. Are you aware of any Federal database which keeps up

with ongoing scams, especially those that are quite frequently the same group or persons or organizations that are doing the scams?

Mr. OLDHAM. I am not. In my role now in advising private companies, I know we call the local law enforcement, usually at the Federal level, to report information, and we rely on them to come back to us with whatever information. But not with a lot of visibility of what is going on behind the scenes.

Mr. KELLY. Are you aware of any program, and this is for any of you, from the SBA or from anyone else that keeps people informed of what the current scams are and the current phishing expeditions and those things? Because quite frequently, people fall victim to something that has been used over and over. Is there anything that keeps people informed where they can go to one source and see that?

Mr. MANKOWSKI. I know that the IRS does release what they consider to be their "Dirty Dozen," which are the top tax frauds that they are suspecting or they are seeing in any given year. What I have seen, especially with a lot of the phishing and the phone calls, is that initially, some of the local news stations were not all that keen on picking up on it, I believe until they started to realize that even some of the people, the top people within the IRS were getting the same phone calls as you and I may be getting, saying that they are about ready to get arrested or your wife is getting arrested or the sheriff is coming to take your car. Now the news stations are broadcasting that the IRS does not make the phone calls. They are getting the word out, which is good, because by getting it out on the news on that end, they are not using any of the budget that is constrained within the IRS at this time.

Chairman CHABOT. The gentleman's time is expired. Thank you.

The gentleman from New Jersey, Mr. Payne, is recognized for 5 minutes.

Mr. PAYNE. Thank you to the Chairman and to the Ranking Member. I appreciate the opportunity to be here, and to all the witnesses, thank you.

I want to ask, would it make sense to coordinate cybersecurity efforts that are focused on small businesses through the SBA? My thought is that if business owners are more informed of computer security techniques and products to secure their networks, we may be able to help curtail some of these cyber attacks. Does that make sense?

Mr. DUNN. Yes, I think so. I think having coordination and a place where really, truly, detailed information about threats and what to do about them is put at and made available to small businesses, would be excellent.

Mr. MANKOWSKI. Just as a comment on that as well, one of the areas as far as coming out with too much specifics as to what you need to do, you are then laying out the playing field for what the criminals need to do to get around your system. That was evident, 2 years ago when the IRS released that no more than three refunds in a calendar year can go into a specific bank account. Through a lot of reverse engineering, they found out that if you start putting a zero before the account number and a second number and a third zero, it was tricking the IRS systems and the banks were dis-

regarding it. It is nice to have the education, but they need to be aware that too much specifics as to what you are doing or what you need to do, you are laying out a simple playing field for the bad guys to just circumvent.

Mr. OLDHAM. I think consolidating information in a place like the SBA would be very helpful. Mr. Dunn had mentioned the FCC planning tool earlier, which is a good start, but that is an agency that has jurisdiction over telecommunication companies. I do not think a small retailer or other companies of that nature would be going to the FCC's website. I think you want to be able to have those resources in a place that folks are willing to call or to search for.

Mr. PAYNE. Sure. I think it would be a natural depository of information. They are already dealing with the agency, so that is something that might make sense.

Unfortunately, even when consumers receive notification of a security breach, many of them do nothing about it or just do not know what to do and the next steps to remedy the breach. What should they do to protect themselves from increased risk of identity theft?

Mr. SNOW. I have got a number of levels of security systems that I have put in place. Number one, I have an external server provider that has a junk mail box. So anything that does not look accurate or looks not quite right, it goes directly into the junk mail. I have an internal system within my network in the building that also looks at that, and that has a separate junk mail file. So if it gets through the first level of protection, it then goes to the second level, at which point the user would have to override that junk mail from both levels. That is one.

Going back to your other question, I think for me as a small business owner, consistency is very important. As the other members mentioned, every state has a different jurisdiction, and for me as a small business owner, I have customers all over the world. If I were ever to be breached and that data was accessed, I would have a number of different jurisdictions to go after and figure out what I need to do. There is a tremendous cost in that.

Mr. DUNN. I think to the point of defense in depth and not relying on any single point of failure, that is pretty key. The concept of having several things that ultimately would have to be bypassed is typically the best approach instead of just having one particular thing.

Mr. OLDHAM. One thing that your question raises is the fact that many Americans are receiving these breach notification letters and they all give the same advice: monitor your accounts, sign up for credit monitoring. It seems like maybe a better way of getting at that is general consumer education as opposed to forcing companies to send out these notifications that many of us receive every week, every month, and doing it maybe a slightly different way that is more impactful for the consumers.

Mr. MANKOWSKI. Finally, from a tax perspective, people, taxpayers, if they do receive one of these breach notifications and find out that they have been a victim of identity theft, they need to not only report it to the three credit agencies, they should also file a specific form with the IRS, which would put them on notice that

they were a victim and that to be careful for a fraudulent tax return coming in from them.

Mr. PAYNE. Thank you, Mr. Chair, I yield back.

Chairman CHABOT. Thank you very much. The gentleman's time is expired.

The gentleman from Missouri, Mr. Luetkemeyer, who is the Vice Chairman of this Committee, is recognized for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Mr. Oldham, quick question for you. We have seen that cyber attacks come in all shapes and sizes and go after businesses of all shapes and sizes, including government agencies, such as the NSA and Office of Personnel Management. While no one thinks that one size can fit all, should not every business and government agency that handles highly sensitive data have some reasonable, but also mandatory, policy and procedure in place for security data against loss and theft?

Mr. OLDHAM. Absolutely there should be policies in place that is standard and mandatory at any government agency that handles sensitive data.

Mr. LUETKEMEYER. It is interesting. Mr. Snow talked about an insurance policy in place. Can you elaborate just a bit, Mr. Snow, with regards to availability and cost and coverages of insurance policies that are out there for cyber attacks? Does it count for your monetary loss or losses to your customers? Does it also cover the liability exposure that you may have to other customers that do business with you?

Mr. SNOW. My understanding is it covers the notification mandates that are required around the country. What would happen, from my perspective, is that I would notify the insurance company, and they would immediately come to my aid in terms of notifying all the customers that their data may have been breached, and also to provide that security to the individual that had the breach in terms of credit reporting and other things. That was my understanding. That was the least expensive of the policies that are out there. There is a whole gamut of different insurance policies that you can get, I am sure covering all the way up to the large liabilities. We have also, on top of that, an umbrella policy that we hope will cover what we feel—in our case we have a $2 million liability policy—we hope that we will not exceed that in any particular breach, but it is an uncertain area.

Mr. LUETKEMEYER. Mr. Oldham, you advise people on the risks that they incur. I would assume you have a pretty good knowledge or extensive knowledge of the availability of these things and how far they go and the costs?

Mr. OLDHAM. Insurance policies. I am not an insurance lawyer, but certainly that comes up in cases. There is a wide range. To the cost in general, it depends on the number of pieces of data, such as affected individuals. If I am advising a client who has to give notifications in 30 different States, that is 30 different statutes that have to be reviewed to do that.

Mr. LUETKEMEYER. So it is basically a policy that is tailored to the individual risk?

Mr. OLDHAM. Yes, again, I am not an insurance lawyer, but when these insurance policies do come up and we have to look at

them, there is a great variation. I am not aware of a standard insurance policy, and I think Mr. Snow, that is probably what your experience was that you were talking about, the marketplace is so new at this point.

Mr. LUETKEMEYER. It seems to me that that is a burgeoning area of need, obviously, and so we will see how it develops.

Along that line, Mr. Dunn, you mentioned a while ago that for small businesses that do business with the government, is there a possibility of compromising government information with those businesses and, therefore, they are exposed for a liability situation? Is there something in the contract that protects them, or do they need to be covering a risk there? How does that work?

Mr. DUNN. I do not know necessarily about a contractual obligation. I think from the perspective of interconnecting systems or share of data there is a liability in either direction. If an attacker was to gain access to a small business that services a government client, the assumption is either the value of the data or some direct connectivity to the government agency may exist.

Mr. LUETKEMEYER. We have an exposure there you need to be careful of, right? As a business, you are going to have to have some sort of, I would think, an insurance policy or some bond of some kind that would protect you in case something went wrong.

Mr. DUNN. I think the whole area of cybersecurity insurance is quite new and fairly immature. I do not know an awful lot about it, but I often wonder what do you have to do in order to be insurable and how do you stay insurable. That may have some kind of compliance or regulatory check.

Mr. LUETKEMEYER. I have always thought that the insurance companies are going to drive this issue because at some point they are the ones that are going to have to insure the issue, and therefore, they are going to demand certain standards. When those standards are out there, they are going to be the ones driving how this is all done.

Mr. Chairman, I yield back the balance of my time.

Chairman CHABOT. Thank you. The gentleman yields back.

The gentleman from New York, Mr. Hanna, who is the Chairman of the Subcommittee on Contracting and Workforce is recognized for 5 minutes.

Mr. HANNA. Thank you. Thank you, Chairman. Thank you all for being here.

I want to talk about a bill—Mr. Payne actually mentioned it inadvertently—I coauthored with Derek Kilmer from Washington. It is the Improving Small Business Cybersecurity Act of 2016. We have 900 small business development agencies around the country. This bill, which would cost, we estimate almost nothing, would authorize and change the Small Business Act and direct these SBDCs to offer cyber support services to small businesses, again, at no additional cost. We would simply be leveraging the SBDCs cyber support services, DHS, and Department of Homeland Security, and the Small Business Administration would simply be required to review current Federal programs and develop, along with the SBDC, a cybersecurity strategy to help in all communities throughout the country. I want to ask you a question, Mr. Dunn, and anyone who wants to weigh in, it sounds like this problem is, at the very least,

a moving target, and it is not just a moving target; it is an intellectually moving target. It is a one-upmanship. It is a constant game, cat-and-mouse type of thing.

You mentioned in your statement, Mr. Dunn, and I apologize for being late to this hearing, training needs to be offered but it tends to be too general. Is it a practical thing to talk to a small business person who may have one or two people and still have enormous impact potential against them. Is it practical in today's world to ask a person to be up to speed in the way they need to be, not just today but going forward. How do you manage that Mr. Oldham, anybody interested in answering that?

Mr. DUNN. The concept is giving them-specific advice on the things that really matter to them. If the example is perhaps they want to offset their email services to a cloud provider, telling them specifically the settings that would be useful to turn on and the benefits is better than just telling them about general awareness concepts about the dangers of email, for example.

Striving for this education around data as being the factor considered the most, you do not have to be up on all the security concepts that currently are happening, but you do have to understand what data you have, the value of it, and then what you should do based on the different value of the different data that you have.

Mr. HANNA. In that sense, Mr. Oldham, anyone, so it is practical to do certain minimal things that help people broadly to limit the possibility of an attack? Mr. Oldham?

Mr. OLDHAM. I think when you step back to the risk management aspect and not just to the zeros and ones, it is very important, as Mr. Dunn said, to focus on what the issue is, and it is usually driven by the types of data. Certain data is more sensitive than other data. Providing high-level guidance that says cybersecurity is important, you should have good cybersecurity, is not helpful to small businesses. It is helpful to provide targeted advice that is practical and granular to their specific situation.

Mr. HANNA. The Small Business Development Centers around the country, the 900, would it be possible for them to establish a basic format that would help the majority of small businesses out there without making it too complicated, difficult, and would it be helpful?

Mr. OLDHAM. I think it would be helpful as long as they have the right expertise going into that guidance. One of the issues that happens in this space is guidance gets put out but it does not evolve with the threat. That is one of the big top-level messages, this threat evolves rapidly, and so do the legal requirements.

Mr. HANNA. If the Small Business Development Centers were able to do this updating, they could be a source in that community, rather than so many randomly small businesses trying to do it on their own and maybe not being entirely effective in that?

Mr. OLDHAM. It sounds very promising. Yes.

Mr. HANNA. Thank you. Chairman, I yield back.

Chairman CHABOT. Thank you. The gentleman yields back.

I want to thank our witnesses for being with us here today. They have helped to clarify just how vulnerable many small businesses and individuals are to cyber attacks. It is a growing and evolving

problem, and you have helped shed some light on what should be done to combat it. For that we thank you very much.

I ask unanimous consent that members have 5 legislative days to submit statements and supporting materials for the record. Without objection, so ordered. If there is no further business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:15 p.m., the Committee was adjourned.]

APPENDIX

Testimony of Rick Snow

Owner

Maine Indoor Karting

On behalf of the National Small Business Association

NSBA
National Small Business Association®

House Small Business Committee

"Small Business and the Federal Government: How Cyber-Attacks Threaten Both"

April 20, 2016

1156 15th Street, N.W., Suite 502
Washington, DC 20005
202-293-8830
www.nsba.biz

Good Morning. Thank you Chairman Chabot, Ranking Member Velázquez and members of the House Small Business Committee for inviting me to testify today on the current state of cybersecurity for small companies and how credit card fraud and phishing scams have impacted my own small business.

My name is Rick Snow and I am the owner of Maine Indoor Karting located in Scarborough, Maine. My wife, Lori, and I started our business in 2003 after being downsized from the financial services industry. We are an indoor entertainment venue with a ¼ mile go-kart track, mini-golf, arcade, and café. We have had as many as 40 employees but since the recession of 2008 we have dropped to less than 20 full and part time employees after losing 35 percent of our gross revenues. We hope to get back to our 2007 gross revenue this year or next.

I am pleased to be here representing the National Small Business Association (NSBA), where I currently serve as a Board of Trustees Member and chair of the Environmental and Regulatory Affairs Committee. NSBA is the nation's oldest small-business advocacy organization, with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted solely to representing the interests of the small businesses which provide almost half of private sector jobs to the economy.

Cybersecurity Landscape

In the last few years, cybersecurity has emerged as one of the most pressing concerns facing both the private and public sectors. Cyber criminals are becoming increasingly sophisticated in their attacks on networks and their attempts to steal personal information that can ultimately lead to severe financial distress. These attacks happen every day and are often completely undetected until well after the damage is done. Some particularly insidious attacks take weeks to slowly infiltrate systems and fully develop. While still other attacks target a third party network, with the hope that the real target will access the infected network.

The terms "data breach" and "identity theft" have truly entered the everyday vernacular of the American public. The enormous breaches at the Office of Personnel Management (OPM) in 2013 and the Internal Revenue Service (IRS) in 2015 in addition to breaches at large nation-wide retailers, grocers and other high-profile incidents have heighted awareness and concerns about these threats. However, heightened public awareness has not stemmed the tide of these threats. There is certainly more to be done to protect all American interests, particularly America's smallest employers, from the dangers these attacks pose.

Private Sector

The threat posed by these attacks to the private sector is enormous, in terms of both the interruption of normal business operations and the direct financial cost of the attack. In a recent report compiling information from 70 different organizations there were almost 80,000 security incidents from 2014-2015 resulting in over 2,122 confirmed data breaches.[1] That is an average of more than 1,000 security incidents a year per organization and more than 300 confirmed data breaches. What is even more alarming is that in almost half of those data breaches, it is not even clear how much data was taken[2], making assessing the damage and repairing it incredibly difficult.

One thing to keep in mind about the private sector is that it is very diverse, whereas the public sector is much more homogenous. In the private sector entities can be differentiated by function structure, industry, and perhaps most importantly, size. This means that there are many more dynamics at play when looking at solutions in the private sector than you may see on the public side. As I will highlight later in my testimony, small businesses like mine have different security challenges and needs than a larger corporation may have when dealing with cybercriminals.

Public Sector

While government agencies are generally structured fairly similarly, it is alarming to me that there have been several high-profile cybersecurity incidents in the past several years spanning multiple agencies. Incidents at both OPM and the IRS have highlighted how much sensitive information the government is entrusted with by the American public. The most recent cybersecurity report published by the Office of Management and Budget (OMB) illustrated the scale of attacks being levied against government agencies. From Oct. 1, 2014 to Sep. 31, 2015, the government reported 77,000 cybersecurity incidents, up 10 percent from the previous year.[3]

Of particular concern to the small-business community is the performance of the U.S. Small Business Administration (SBA) in this report. Although, there has been a marked decline in policy violations at the agency in the past three fiscal years, this report indicated that in FY 2015, there were three times more incidents involving suspicious network activity than in FY 2014.[4] It is further concerning that SBA continues to lag behind other agencies in certain email screening

---

[1] Verizon, *2015 Data Breach Investigations Report* 1 [hereinafter *DBIR*], *available at* http://www.verizonenterprise.com/DBIR/2015/.

[2] *Id.* at 3.

[3] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Modernization Act* 5 (2016) [hereinafter OMB Report], *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.

[4] *Id* at 59.

and phishing prevention programs.[5] The report indicates the SBA email systems simply do not check sender verification when receiving messages from outside the network[6] and use of content filtering programs to prevent access to websites posing cyber threats is nonexistent.[7] SBA has and handles sensitive information concerning millions of small businesses, and the results of a large-scale breach within the agency could be catastrophic for the small-business community. It is quite worrisome to me that the very federal agency tasked with supporting small businesses lacks the essential resources to defend us against cybercriminals.

Breaches at the government level, particularly at the IRS, are troubling for small-business owners because the financial stability of the owner is inextricably tied to the stability of the small business and vice versa. A financial loss on the personal front can seriously impair the functioning of the business while a loss for the business can potentially be detrimental to the owner and their family. These are the dangers that small-business owners face and they are very different than those faced by larger companies. If the federal government cannot protect its networks and data from cyberattacks with almost unlimited resources at its disposal, how can we expect America's small businesses to do so?

NSBA and its members are mindful of the work of Congress in recently passing cybersecurity legislation and applaud their efforts. Facilitating dialogue between the public and private sector about threats is terribly important. There needs to be continued thought given as to how to make this dialogue truly beneficial for small businesses. Any federal discussion on cybersecurity or development of a private-public partnership or advisory board must include representatives of small business. NSBA has long urged Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of online data and financials, but caution against a knee-jerk reaction that would unfairly place a disproportionate burden on America's small firms.

Congress also needs to realize that most of these attacks move alarmingly fast. Approximately 75 percent of attacks spread from the victim 0 to victim 1 in less than a day, while almost 40 percent of them do so within 1 hour.[8] Keeping in mind the infrastructural limitations of small businesses, it is crucial Congress finds ways to keep them abreast of these threats by providing clear, simple steps companies can follow when their data is breached and balancing the need for greater information sharing with privacy rights.

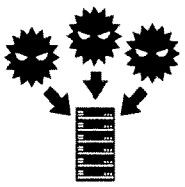
---

[5] *Id* at 69, 72, 75.
[6] *Id.* 69.
[7] *Id.* at 75.
[8] *DBIR*, at 11.

Small-Business Perspective

Given the increasingly commonplace occurrence of hacking and cyber-crimes, coupled with the fact that, over the past few years in a difficult economy, small-business owners are handling more of their firm's IT operations, cybersecurity is a growing concern for small business. Even a simple cyber attack can effectively destroy a small business.

Has your business been the victim of a cyber-attack (i.e. computer virus, malware/spyware, website hack, credit card or banking hack or trojan, etc.)?



	DEC. 2015	DEC. 2014
Never	58%	50%
Only once	17%	16%
2 to 5 times	21%	28%
More than 5 times	4%	6%

What was the nature of the cyber-attack? (check all that apply)

My computers were hacked	34%
My credit card information was stolen	31%
My website was hacked	17%
Our entire network was hacked	13%
My bank account was hacked	10%
My company information was hacked from a third-party (i.e.: insurance company, accounting company, etc...)	7%
Our cloud data was hacked	2%
Other	16%

These attacks are startlingly becoming more common among small businesses. In a recent NSBA survey, 42 percent of members indicated that they had been the victim of cyber attack.[9] In almost a third of those attacks on NSBA members, credit card information was stolen. In 13 percent of the attacks the entire network was compromised and in 10 percent a bank account was hacked.

The NSBA Year-End Economic Report emphasizes the fact that in an increasingly technology-reliant global marketplace, cybersecurity issues and vulnerabilities can bring commerce to a screeching halt. In almost half of the attacks, there was an interruption in service.[10]

[9] National Small Business Association, *2015 Year-End Economic Report* 12 *available at,* http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
[10] *Id.* at 13.

On average, how long did it take to resolve cyber attacks?

	DEC. 2015	DEC. 2014	AUG. 2013
Less than 1 day	24%	30%	38%
Between 1 - 3 days	34%	34%	40%
Between 3 - 7 days	15%	14%	11%
More than a week	10%	9%	7%
More than two weeks	16%	13%	5%

In 75 percent of the cases, it took more than a day for the issue to be resolved, and 26 percent of the time it took more than a week to resolve.[11] This is in stark contrast to larger companies where an attack may not even slow down operations while sophisticated IT departments repair the damages. But many small businesses are not able to have dedicated IT departments and still others have to outsource IT functions or assign these duties to an employee as a secondary function. In fact, in 2013, 40 percent of business owners were handling IT personally and only 24 percent were outsourcing the function.

For those owners handling it themselves, it is certainly expected that resolving incidents will require research, training, trial and error, and a great deal of time away from the core functions of the business—acting as accountant, benefits coordinator, attorney, and personnel administrator. Simply outsourcing the function is not necessarily a silver bullet either. It can be cost prohibitive for some businesses and there are also issues in expected service delays. Simply put, a small business might not be high on the IT service provider's list of priorities if there is a systemic problem, even though such a firm is more likely to have the experience and technical expertise to resolve the issue quickly. The economies of scale which make retaining in-house IT professionals efficient for larger companies simply do not exist for small businesses and thus creates serious unique challenges to the smallest ones.

Although, small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats. However, on average NSBA members indicated that each attack costs them over $7,000. Additionally, when money was stolen from bank accounts as a result of these attacks, the average amount stolen was $32,000. Small businesses often operate on very tight profit margins and seldom carry a lot of excess cash. These losses can be devastating to businesses in those circumstances.

[11] *Id.*

It is unfortunate that the resource limitations illustrated above make small businesses a greater target for attacks than larger companies. Fewer IT resources and dedicated staff mean that cyberattacks may require less sophistication and perhaps even more importantly, garner slower reaction time. In many cases, small businesses without sophisticated monitoring equipment or contractors may not even know they have been the victim until days after an attack. The reality is that those cybercriminals are aware of these limitations and at times specifically target small businesses because of them.

Phishing

Although cyber attacks through "hacking" and viruses are common, phishing continues to be one of the most damaging forms of attacks against small businesses. Phishing is generally when a fraudster sends messages impersonating a business or organization to solicit sensitive information from the receiver—often citing an urgent need to login to an account or provide other vital information. In prior years many of these attempts where rudimentary and conspicuous. However, recently they have become increasingly sophisticated, many containing carefully crafted emails mimicking those of the impersonated bank or other trusted institution or even directing the user to a clone of the impersonated businesses website. Attacks of this nature have increased from about 2 percent of cyber attacks in 2010 to 20 percent in 2014.[12]

Success rates of these phishing campaigns have varied, but in some situations 23 percent of recipients are opening the phishing messages and 11 percent actually click on attachments.[13] These campaigns operate incredibly quickly, often those who open a phishing email do so within an hour of it being received, in many cases because the scams purport to require emergency action. In some tests, the first response to a phishing campaign came in under two minutes.[14] With the ability of employees to work remotely at all hours with constant access to email and other vital company information, this means that a network or sensitive information could be compromised almost instantaneously, at any time. A sobering and terrifying thought for small-business owners. Phishing attempts also continue to be the primary method of cybercriminals who attempt to exploit government systems as well, so small-business owners certainly are not alone in their concerns.[15]

Because the human element and the fear of inaction that these emails are intended to illicit will always compromise some, it is generally accepted that the best way to prevent these attacks from succeeding is to totally prevent phishing messages from arriving at an employee's inbox. This

[12] *DBIR*, at 5.
[13] *Id* at 13.
[14] *Id.*
[15] *OMB Report*, at 22.

cuts against small businesses again because of the limitation on resources. Sophisticated software necessary to filter these messages and detect when the messages succeed is not available to all businesses—making the attack on a small business more likely. In a larger company, very few people would even have access to sensitive information. However, in a small business, proportionally more people with less training would have access to the information, making the number of potential targets more tempting to cybercriminals.

Phishing is also particularly dangerous to small businesses because business accounts do not have the same level of protections and guarantees against loss and theft as those provided to consumers. Business accounts are governed by the Uniform Commercial Code, which does not hold banks liable for unauthorized payments as long as the bank employs a commercially reasonable method of providing security. This means that a small business whose funds are stolen from its account is not guaranteed to have the losses covered. Many small-business owners do not know this until it is too late and never recover stolen funds.

Bearing all this in mind, my experiences with cyber threats should not come as much of a surprised.

Maine Indoor Karting

When I started my business I had the naïve expectation that I would be able to follow my passion and race go-karts with the help of my wife and a few close friends. I had no idea of the demands that are placed on a small-business owner. When you own your own business, everything is your responsibility. I had to become an expert in human resources, insurance, banking, theft, employee psychology, plumbing, electrical work, restaurant management, regulations and advocacy.

My first introduction to the dark side of small business-ownership came three months after opening and we discovered that someone was removing cash from our drawer, after two months and losing an estimated $50,000 we discovered the culprit and let that individual go. I then went through the expense of installing an expensive camera system to work with the installed burglar alarm system. It is unfortunate that I had to take such extreme measures to simply protect my business and to think that it would not be the only or last time I had to take measures to protect my small business from theft.

Phishing can happen to anyone, phishing attacks are meant to scare you and make you act without thinking, given the right circumstances, anyone can be lured by them. I am certainly no exception. I was busy working at my desk one day, when I received an alert email from my bank that there had been a suspicious online attempt to gain access. The email urged me to

immediately log into my account to confirm that it was an unauthorized attempt. The link provided in the email looked identical to the log on page for my bank. Frantic that my business could be loosing all of its funds, I stupidly did just that. As soon as I typed my password I realized that I had been phished. I had to drop my work and race to the local branch of my bank and explain what happened. The bank required that I then set up a new account, which took several hours.

Additionally, I had to order new checks and debit cards for myself, wife, and three staff members authorized to use company cards. It took about a week to rush the new checks and debit cards to us. Since we use the cards and checks for all our bills and local purchases for the events we put on for our customers, I had to either use our company credit card (with a line of credit of 24 percent interest) or my own credit card which I would then have to reimburse myself when the new checks arrived. Situations like this blur the lines between personal finance and that of my small business. The cost was roughly $250 for the new checks and rush order and overnight shipping not to mention the delays and disruptions to my business. It took my wife an additional day to update our entire auto bill paying with the new account numbers and another day on the phone to update the payroll company. Since she runs the day- to-day operations of the business, she had a very stressful week trying to keep up with the regular routine and update all our vendors. However, I know that it could have been much worse, and soon thereafter, I experienced how much worse it could really be.

Two weeks later I was working late, like most evenings, and I decided to check on our business for that day. I logged into our bank accounts, and to my utter horror, I found that my balance was zero. This was a pay day, and I was terrified that the paychecks that were issued that day would not clear. We were supporting a number of families, many of which live paycheck-to-paycheck and could not have made it without the paycheck we issued them that day. I was also very worried about our business' reputation since a restaurant nearby had just bounced their paychecks and the company never recovered from the bad publicity they received from not making their payroll. I quickly discovered that three wire transfers were made that night to three different banks around the country totaling $15,000. Fortunately the payroll company had debited the new account the night before so I knew our employees would be paid.

I then spent the rest of the night trying to get a hold of someone in my bank to stop the wire transfers and recover the money. Because it was so late, none of the banks in my region were open. I was luckily able to get in touch with one bank still open in Washington State. I had to be at the bank first thing the next morning, but I was able to stop the wire transfers. However, I had to than spend another day away from work opening a new account and going through the process—that I had just done—of getting all new cards and ordering new checks. Again, there were disruptions in my ability to make purchases for business. My poor wife had to spend

another week going through the same process she did just two weeks earlier. My wife, who is also our business' book keeper, spent the better part of two weeks away from her normal duties because of this phishing incident. She also told me that if this happened again, I would no longer have a wife or a book keeper. To this day no one knows for sure how the cybercriminal was able to gain access to the new accounts.

My bank told me that this was a standard phishing loss and that I was lucky that I discovered it before 48 hours had lapsed so no money was actually stolen. My business accounts are not protected against theft the way that my personal accounts would be. Other than being out the cost of the two new check books and the man hours and a lost night of sleep I was lucky. I also discovered that there was going to be no one at the receiving banks to arrest the person claiming the stolen funds.

Since then, my wife and I have had our personal credit cards stolen three different times. Like most small businesses the line between our personal finances and that of our business is often blurred, we sometimes have to use our personal credit to support slow times in the business cycle.

The first time my card information was stolen, I received a call from MasterCard security asking me if I was in Japan, I was at home and most certainly not in Japan. After confirming both my wife and I had our credit cards, they informed us that someone had used our card the night before in Japan to make $14,000 worth of purchases and that our cards would be frozen until new ones arrived. Fortunately, the money was frozen on our account and we had to fill out a notarized statement to state that we were not the individuals making the purchases. We were told that we should have the money back in our account in 30 days. This was our Cash Management account so we had to use the margin of our stocks and bonds to support us for the rest of that month. I was later told that someone had cloned our card and used it overseas.

The next time our card was stolen was during the Hannaford loss where it is estimated that seven million card numbers were stolen. As a precaution we were told by our issuing bank that we should replace any cards that we use at Hannaford. We use that company card for both our personal food supply and also use them for our catering needs at the track. Our bank was able to reissue the debit cards for our business that day at the local branch, but our personal cards would need to be overnighted from Morgan Stanley. That was the most frustrating for us because the new card was going to be overnighted to us while we were out-of-town. Because of horrible logistics we had no use of our card for the week we traveled and had to go to a Fed Ex office in Florida to finally pick up our cards.

The most recent was just a couple of weeks ago when my brand new chip card was used in Long Island to purchase $300 worth of products at a Bed Bath and Beyond. Again, I was out of credit card use for a week waiting for my new card.

In all of my cases, I have been lucky that I was not out the money that was stolen. It cost me a lot of my time and frustration to deal with all these attempts and the merchandise purchased with my fraudulent cards was never recovered and someone had to absorb those costs. Now that the laws have changed if I do not use the chips for processing my sales at my business, I will be responsible for those losses. For me, I have now implemented a policy that I hope prevents another phishing expedition using server based software for spam and a second computer based security system to identify junk mail. I pay $500 per year for the software system and the server based system is part of my IT company's package.

Any of these attempts could have ended my business if I was not able to recover the money. Most small businesses do not have a significant cushion to absorb these types of losses, and we are no different. Losing thousands of dollars at bad time could make a significant difference for both me and my business and for my employees.

Conclusion

As small businesses become increasingly dependent on services and applications that connect to the internet, they also become a larger target for cybercriminals looking to exploit vulnerabilities to steal money and credit card credentials, intellectual property, personally identifiable information as well possibly destroy data and disrupt operations. These threats are very real and immediate. In fact, ninety four percent of small-business owners indicate that they are concerned about being targeted by cyber attacks. For many small firms, a cybersecurity incident could lead to an entire network being down for many days until the full extent of the problem is known and then fixed. Not to mention that a highly public breach could also damage the business's brand and lead to long-term loss of income.

This is the ongoing threat of the internet age, as more and more small businesses rely on web-based products and services, and it will only persist and evolve as long as the internet continues to facilitate commerce in the global economy. It is unlikely that there will be one solution to stop all of the attacks. In fact, slowing and preventing these attacks will most likely require an ongoing process to identify new threats, vulnerabilities and ultimately solutions. NSBA urges Congress and this committee to always bear in mind the unique challenges that small businesses face and continue to include the small-business community in that process.

Thank you for allowing me to testify before the committee today. I would be happy to answer any questions you might have for me.

Testimony of Rick Snow, Maine Indoor Karting
On Behalf of the National Small Business Association

nccgroup

Testimony of

KEVIN DUNN
TECHNICAL VICE PRESIDENT
PRACTICE DIRECTOR, SECURITY DEFENSE OPERATIONS

NCC GROUP SECURITY SERVICES, INC

Before the

UNITED STATES HOUSE OF REPRESENTATIVES
SMALL BUSINESS COMMITTEE

On

SMALL BUSINESS AND THE FEDERAL GOVERNMENT:
HOW CYBER-ATTACKS THREATEN BOTH

April 20, 2016

nccgroup

Good morning Mr. Chairman, Ranking Member Velazquez and other esteemed members of the Committee. Thank you for the opportunity to testify today. My name is Kevin Dunn, Technical Vice President for NCC Group Security Services.

For the last fifteen years I have dedicated my career to carrying out cybersecurity attacks against private companies and government organizations. I am not a criminal; I am a 'Penetration Tester'.

Through our actions in this highly specialized field, my colleagues and I determine ways to break into organizations via cyber and physical means. Specifically, we are hired to identify vulnerabilities that allow a company's security to be compromised.

This exercise subsequently allows us to provide customized advice to our clients, detailing the short-term and long-term actions they should take to reduce their susceptibility to attack.

My testimony today will focus on four areas:

1. The Strengths & Weaknesses of Cybersecurity Training
2. Increasing Security when using Cloud Service Providers
3. The Potential Impact of Small Business Security on the Government
4. The Benefits of a Data-Driven Risk Model

The Strengths & Weaknesses of Cybersecurity Training

To evaluate the state of high-level cybersecurity training designed for small businesses let's explore two examples: training provided by the U.S Small Business Administration and the Federal Communications Commission.

Through these trainings, small businesses are able to gain awareness of important cybersecurity threats such as the dangers associated with phishing emails, malicious websites, malware, ransomware, and the typical motivations of attackers. This information provides an ample start for educating small businesses in a general awareness capacity, and extends to providing cybersecurity tips for the major areas of concern.

However, the training and guidelines are high-level in nature, and lack the depth of information needed to convert directly into hands-on actions. In the world of small business IT support, where efforts are typically coordinated by owner-operators, this information may not be comprehensive enough to make a worthwhile difference beyond providing general education.

Cybersecurity training for small businesses should provide direct information in the form of 'how-to' guides, answering the need for specific guidance in addition to high-level awareness.

Increasing Security when using Cloud Service Providers

Many small businesses use Cloud Service Providers to implement important services like email, file storage, and data backup. This often unburdens the IT administration overhead from small business owner-operators, or small businesses with a one or two-person IT team.

The use of third party Cloud Service Providers is typically a positive security move for small businesses. The attention to security from the major providers in this space affords a number of features that greatly increase the security of data for a small business. However, it should be noted that there are additional features that should be enabled to make attacks harder for adversaries; these features are often not enabled by default.

Chief among these is the use of multifactor authentication. The majority of major online services now support the use of multifactor authentication, using at least SMS messages to a cell phone as a means of 'out-of-band' authentication. But despite this inexpensive option, it is often overlooked by organizations that use Cloud services, relying instead on 'single factor authentication' in the form of usernames and passwords.

Using multifactor authentication, that makes use of an out-of-band hardware token, would greatly improve security operations for small businesses using Cloud services.

The Potential Impact of Small Business Security on the Government

The impact of a small businesses on the government should be considered in at least two key ways. The first concerns the direct and indirect connectivity between a small business and a Government Network. The second concerns small businesses in the government supply chain.

A small business with a direct connection to a government network is likely a rare occurrence, but in such a scenario if the small business is compromised sufficiently, an attacker's ability to traverse to a government network could be a simple task. However, examples of indirect connectivity are more common and are typically data-based in nature. When government users consume the services of a small business, their usernames, passwords, personal information or other data could be used in a subsequent attack against government systems if extracted from a compromised small business system.

The second area to consider is when a small business is in some way part of the supply chain to a government department or agency. The most typical examples of this are where a small business develops software or hardware that is subsequently installed on government networks.

In all of these examples, if the small business is compromised by a targeted attacker, it could be used as a conduit for gaining access to government systems.

The Benefits of a Data-Driven Risk Model

Finally, a good way to think about security, and a means to ensure that the approaches chosen to secure your organization are 'fit for purpose', is to think first about the data that you care about.

Considering the data first is an excellent approach, and one that is advised in the FCC's Small Business Cyber Planner tool. However, too few organizations actually consider their data, or subsequently plan security around the value of different data types. Even fewer organizations consider what will happen when (not if), an attacker gains access to their data.

Using a data-centric risk management model will allow small businesses to focus their security attention where they need it most.

Thank you again for this opportunity to address the Committee; I will be happy to answer any questions.

Statement of
Nicholas A. Oldham

Counsel
King & Spalding LLP

before the
U.S. House of Representatives
Small Business Committee

April 20, 2016

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to appear before you today.[1]

I have been involved in cyber issues for many years—as a former federal prosecutor at the U.S. Department of Justice and now as an attorney with King & Spalding. In my practice, I counsel clients, both large and small, on the legal aspects of cybersecurity risk management.

Today, I focus my testimony on the cybersecurity landscape for small businesses, and on three areas of particular concern—the cybersecurity education gap, the need for cybersecurity initiatives to be calibrated for small businesses, and the need to clarify and simplify the current regulatory environment.

Background

We are living in exciting times. Digital assets and connected systems have generated new products and services, redefining how business is conducted and services delivered. But the truth is that we are only at the beginning of the beginning when it comes to understanding the implications of our reliance on this interconnectivity and the dangers that cyber threats present.

Our *interconnectivity* is growing at an astonishing rate, with some estimates that there will be as many as 50 billion devices connected to the Internet by 2020. As a result, we are marching toward an infinitely connected world: always online, our information moving from network to network and device to device.

Partly as a result of this interconnectivity, businesses are gathering and utilizing an ever-growing amount of information to improve their business practices and better serve their customers. Today, every online communication, transaction, and anything else you can think of can be captured and stored, and then transmitted electronically anywhere and at anytime. This interconnectivity, especially including the Internet of Things, holds tremendous promise for consumers and companies.

It also creates new challenges in terms of *cybersecurity* because anything connected to the Internet can be hacked. Cyber threats vary from the technologically sophisticated to the surprisingly low tech methods such as "social engineering" and spear phishing. A recent RAND Corporation study found that over a quarter of American consumers received a notice that their data was stolen within the past year alone. Forbes recently reported that cyber-attacks cost businesses an estimated $400-500 billion per year, and because many cyber-attacks are not reported, it is believed that the real number is significantly higher. These reports underscore the significant costs of preparing for, responding to, and recovering from cyber incidents.

Where do small businesses fit in this landscape? The interconnected world enables small businesses to develop new products

[1] The views and opinions expressed in this statement are mine and do not necessarily reflect the views or opinions of King & Spalding or any of its clients.

and services and compete across the globe. However, growing cyber threats presents greater challenges to the same small businesses, which can lack the tools needed to effectively cope with the growing danger.

Small businesses are appealing targets. Small businesses often have more digital assets than individual consumers, but their resources may not allow for the same level of focus on cybersecurity as large companies.

Businesses of all sizes need adequate cybersecurity education, but it can be difficult for small businesses to find the right information and training.

Small businesses also often feel the impact of cyber threats differently than large companies. Establishing effective cybersecurity and incident response mechanisms is complicated and can be expensive. When any business implements mitigation measures or responds to a cyber incident, it can lost significant time and money. The costs can sink a small business. Small businesses get burned at both ends—they are less likely to have the resources to prevent breaches and they also may have fewer resources to respond to those breaches.

From Cyber Threat Awareness to Cyber Risk Management

In June 2011, various Committees in both the House and Senate held hearings regarding data breaches at Sony and Epsilon Data Management. In March 2012, then-FBI Director Mueller gave a now famous speech at the RSA Conference in San Francisco. His oft repeated quote is that "there are only two types of companies: those that have been hacked and those that will be." These events were key, early moments that helped raise awareness of cyber threats. We have much farther to go in terms of awareness and, perhaps more importantly, companies need to move from awareness to expertise in managing the new normal of cyber threats.

As a lawyer, I do not manage corporate networks or conduct vulnerability testing. Rather, I believe that cybersecurity is as much a people and process issue as it is a technical issue. I focus on the people and process side of the equation, addressing the legal and business cybersecurity risks faced by companies including cybersecurity risk governance, compliance, and incident response processes. I also help companies comply with breach notification obligations, interact with various regulators, and manage their responses to regulatory actions or litigation. The legal and business costs, including compliance costs, drain on employee time and morale, and reputational damage, can be significant.

The Cybersecurity Education Gap

Before spending precious resources on increasing cybersecurity measures, it is natural for small businesses to carefully weigh the cost of putting new measures into place versus the cost to the company of the inevitable cyber incident if it does not take action. Because of the enormous potential costs of a cyber incident, which is difficult to quantify, companies may find that it is far more expen-

sive to not implement basic security measures. The problem here is that there is a cybersecurity education gap: small businesses may not be able to get the information they need to properly assess and mitigate these costs.

Bridging this education gap can be difficult for small businesses, especially those that lack the resources to hire specialized employees or cybersecurity experts. Basic resources are available online, but even where they provide crucial information, they can be difficult to find, are rarely updated, or are inadequate.

On the legal compliance front, the Federal Trade Commission recently released a new web-based tool for developers who make health-related apps. The tool asks developers a series of 10 high-level, yes or no questions related to their apps covering topics such as the apps' functions, data they collect, and the services they provide. Then, based on the answers to the high-level questions, the tool identifies four potentially applicable federal laws. While useful as a starting point for introducing and orienting developers and other healthcare industry players to the legal thicket affecting health apps, the tool provides high-level guidance on the basics of only a few relevant laws.

The FTC's tool is one example of an approach geared toward educating the public on legal compliance. The tool is somewhat promising, but does not cover all relevant laws and does little more than point the developers to summaries of the relevant language. This approach, however, could go a long way toward helping small businesses stay informed on cybersecurity legal best practices, provided such tools are expanded to cover a broader set of laws and give more specific, timely information.

In many ways, cyber threats have analogs to traditional crime. Ransomware is cyber extortion, spear phishing is nothing more than a con artist taking advantage of the ubiquity of e-mail. Hackers, moreover, are like burglars. They use their "gloves," "dark clothes," and "tools" to get inside a network, stealing digital loot along the way. In the traditional crime scenarios, small businesses would likely call the local police department for best practices in preventing these crimes or responding to them. In the digital crime scenarios, there is no one logical place to call. The government may have a role in bridging the cybersecurity education gap by encouraging the development of cybersecurity education resources and connecting them to those who need them in the private sector.

Existing Programs Are Not Geared Toward Small Businesses

Many of the cybersecurity initiatives receiving the most attention are not necessarily tailored to take into account the realities of small business owners. Standards seem to be coalescing around the NIST Cybersecurity Framework in some areas, for example, which is a promising development. This has the potential for simplifying the landscape for small and large businesses alike.

The current iteration of the NIST Framework, however, is not particularly geared toward the needs of small businesses. The

Framework itself can be difficult and expensive to understand and implement regardless of business size, and until it is better tailored to small businesses, for some of them it may just be one more program that they cannot afford to keep up with. Perhaps more importantly, a small business might become subject to a cybersecurity framework by virtue of its contractual relationship with a partner that passes its cybersecurity obligations through its supply chain. In this case, the small business might agree to obligations under the cybersecurity framework without the same level of vetting it might undertake if it were adopting the framework from scratch, and thereby inadvertently expose itself to significant liabilities and expose itself and its partners to significant cyber risks.

While good cyber hygiene is important, to improve the NIST Framework, and similar programs and policies, the government should make a serious effort to increase the involvement of small business owners in all phases of the legislative and rule-making process. Until small business concerns are fully baked into these standards, they could face serious challenges of adoption.

The Current Regulatory Regime Is Difficult to Navigate

The current regulatory regime for cybersecurity presents additional difficulties for small businesses, who will inevitably struggle to determine both (1) what cybersecurity measures they are required to enact, and (2) when a breach or attack does occur, what procedure the law requires them to follow.

There are currently 51 different state or territory laws that pertain to the notifications a company that has been the victim of a data breach provide to its customers. They are inconsistent with each other in a variety of ways. Additionally, several states have enacted laws requiring companies to put "reasonable security measures" in place. What "reasonable" means in this context is evolving and can differ by jurisdiction and industry. I have seen a growing number of federal regulatory agencies stepping into the same space.

The cost of ensuring compliance with laws for any company is enormous even before taking into account the cost of litigation and reputation damage if a breach does occur. Small businesses in particular are vulnerable to these costs because they can consume a much larger proportion of their available funds. Small businesses would benefit from a public sector approach that lowers the cost of compliance and the cost of implementing best practices.

In short, there is a need to clarify and simplify what companies must do. Because of the complicated and evolving landscape, the on-the-ground expertise of the private sector must necessarily play an important role in these efforts.

Thank you for the opportunity to testify before you today. I look forward to your questions.

NATIONAL CONFERENCE OF CPA PRACTITIONERS

22 Jericho Turnpike, Suite 110 *T: 516-333-8282*

Mineola, NY 11501 *F: 516-333-4099*

Chairman Chabot, Ranking Member Velazquez and members of the Committee, thank you for inviting me to testify today. My name is Stephen Mankowski. I am a Certified Public Accountant, Executive Vice President of the National Conference of CPA Practitioners, **(NCCPAP - the countries' second largest CPA organization)** and a member of the American Institute of CPAs (AICPA). **NCCPAP** is a professional organization that advocates on issues that affect Certified Public Accountants in public practice and their small business and individual clients located throughout the United States. **NCCPAP** members serve more than one million business and individual clients and are in continual communication with regulatory bodies to keep them apprised of the needs of the local CPA practitioner and its clients. Accompanying me is Mr. Sanford Zinman, National Tax Policy Chair of **NCCPAP.**

My firm, E.P. Caine & Associates CPA, LLC, has been preparing tax returns for over 30 years. My firm annually prepares well over 2,000 small business and individual tax returns as well as sales tax returns, payroll tax returns, highway use tax returns and Forms W2 and Forms 1099 informational returns. We are in the trenches with clients discussing their tax, financial and personal issues, and the impact events and proposed tax law changes may have on them. Although our clients are mostly in the Pennsylvania, New York, New Jersey and Delaware areas, we serve clients in over 30 states and also provide services to clients in Canada and Europe. In this respect our practice is the same as many members of **NCCPAP** and other smaller CPA firms throughout the United States.

NCCPAP has been at the forefront of identity theft issues through our advocacy and testimony at prior hearings dealing with ID theft in June 2012. The initial hearings focused on the refund scams that were prevalent at the time, such as Mo Money. **NCCPAP** has remained vigilant on the topic and has been discussing these issues annually when our members meet with Congress and their staff and with IRS representatives. Our members have helped guide numerous taxpayers who have been victims of ID theft to navigate through the IRS to minimize the risk of further consequences.

ID theft has been growing exponentially for years. It seems that no matter what controls are put in place, criminals have better and more focused resources to circumvent these safeguards. All businesses are at risk, from the largest to the smallest. Weekly, we are hearing about the latest business to be a victim of some level of cybercrime or ID theft. Mr. Richard Snow, who is also on the panel of witnesses today, has been a victim.

All businesses are at risk, but CPA firms and tax practitioners are at a greater risk. The IRS reminds tax preparers that they must be vigilant with their system integrity. The criminals are aware that the "prize" for breaching tax practitioner systems could yield them not only names and social security numbers, but also several years of earnings as well as bank information and dates of birth. Thus, the IRS recommends that tax preparers create a security plan. IRS Publication 4557, Safeguarding Taxpayer Data, provides suggestions and a checklist. My firm has reviewed the Publication, continually trains our staff and, along with our IT consultants, monitors our information and controls to ensure that our offices not only meet but exceed these suggestions. Our network logs usage form all users and is monitored to ensure no unauthorized access. This includes staff with remote access to our server. We also require a user id and passwords to gain access to all of our software packages. Not all firms have been as fortunate regarding cyber security. Two Midwestern firms were compromised this tax season and had fraudulent returns filed through their electronic filing identification number (EFIN).

I was able to speak with a partner at one of the affected firms. They were under the impression that their systems were secure. However, the breach occurred after installing a new copier system that had not been properly secured within their network. Once they determined that they did in fact have a breach, they attempted to contact the IRS. Unfortunately, there is no easy means to identify the proper area within the IRS to contact. Ultimately, it took nearly one month for a response from the IRS.

Ensuring the security of client data has been and remains the goal of my firm and we take that task very seriously. Although our software has the ability to auto-generate the PINs for electronic filing (EF PIN), we became aware that the EF PIN was using a portion of the taxpayer SSN. We have opted to not use this part of our software and have chosen to manually enter the EF PIN. Some tax software packages use a random five-digit number and we have suggested our software provider offers the same option. Taxpayers are also able to obtain their own specific EF PIN through the IRS website through the entry of select information. Currently, this system is too new to ascertain the true effectiveness of the program; however, concerns exist as to whether the return would reject if this number was not used or what would happen if the taxpayer lost this number. It is not clear if there is a mechanism to retrieve the number from the IRS.

Practitioners are also reminded to protect their EFIN. The IRS suggests practitioners log into e-services on a regular basis and verify the number of returns processed for their EFIN. While the number probably will not be exact due to the timing of return processing and updating of this service, significant differences could be a cause for alarm. Practitioners should contact the IRS e-Help Desk immediately if the difference is excessive. At the beginning of this filing season, the tax software community requested that tax practitioners update their EFIN authorization letter before they start using their EFIN. This is just another step in preventing potential unauthorized access to a practitioner EFIN. While in many

cases the timing of this request might not have occurred at the most opportune time, such as when the first returns were to be filed, it sent a signal to the practitioner community that the software vendors understood the issues and were working in conjunction with practitioners to address ID theft.

While firms that electronically submit tax returns are required to obtain an EFIN from the IRS, paid preparers initially included their social security number on tax returns and in 1999 were first offered the ability to use a Preparer Tax Identification Number (PTIN). The requirement to include the preparer's firm information, which includes their employer identification number, began in 1978. Given the risks of firm ID theft, why has the IRS not adopted a firm PTIN?

There are two primary reasons that criminals attempt to breach systems—the challenge and/or for the information contained in the systems, both reasons for IRS action. The IRS has been transitioning to modern technology within its network protocols to enhance safeguards. During this transition, the IRS has encountered many of the same compatibility concerns that affect most businesses. As a CPA, I became aware of this when the IRS announced the planned retirement of the Disclosure Authorization (DA) and Electronic Account Resolution (EAR) options on IRS e-services in August 2013. When the tax practitioner community complained that the elimination of these options would have a significant impact on their practices, we were told that the platform on which these services were designed was not compatible with the new system architecture and the initial costs to rewrite the programming was excessive. The IRS has looked at a relaunch of these services in the future, but the added authentications might make the systems overly burdensome.

In March 2015, one tax software vendor had its electronic processing systems compromised to the extent that the state of Minnesota and subsequently all states temporarily ceased accepting electronically filed returns from that vendor. One positive result of this situation was the formation of the IRS Commissioner's Security Summit, which initially included representatives from state governments, banking and the software community. This group approach was a positive signal from the IRS that the issues of identity theft and data security required a multi-faceted approach to work at stemming the increases in data security and ID theft. Their initial focus was addressing and stopping suspected fraudulent returns through the implementation of protocols to address issues with tax returns before processing and during the initial processing. According to a recent General Accounting Office (GAO) report, it is estimated that during the 2014 filing season the IRS paid approximately $3.1 billion in fraudulent refunds while preventing $22.5 billion. This was before the creation of the Security Summit.

In its initial year, the Summit estimates that it has prevented in excess of three million fraudulent returns from being processed and refunds issued during the 2015 filing season, but many fraudulent returns are still getting through. The Summit has not been ex-

panded to include tax practitioners. The next level of focus needs to be on securing the refund process. According to Senator Wyden, the IT budget within the IRS is now operating at a level lower than it was six years ago due to budget cuts. The criminals, however, have ample cash and sophisticated systems. They continually attempt to reverse engineer the security measures implemented by the IRS. One recent instance occurred when the IRS announced that only three IRS refunds would be able to be direct deposited into a bank account in any calendar year. It was determined that adding zeros before the account number would trick the IRS systems to think it was a different account number and allow the refunds to be deposited. It satisfied the IRS systems while being disregarded by the financial institutions. This was a case that I believe the IRS learned a valuable lesson—while you can publicly address the solutions being implemented, you should not provide the specifics. The limitation of refunds was designed as a deterrent, but ultimately only served as a means of preventing tax preparers from illegally collecting the fees from a taxpayer refund.

The timing of the receipt of data by the IRS often comes into question. Often fraudulent returns are submitted with refunds transmitted long before the data needed to verify the income and the tax withholding is received by the IRS. Businesses filing Forms W-2 on paper are required to submit the data by the end of February, while electronic filers had an additional 30 days. In addition, an automatic 30-day extension had been available. Because of the delay in submission of these information returns, the criminals have begun filing fraudulent W-2s. In an effort to counter this practice, Congress has removed the automatic extension for filing paper or electronic information returns. However, a time discrepancy still remained. The Protecting Americans from Tax Hikes Act of 2015 (PATH) clarified and simplified these dates. For tax years beginning in 2016, Forms W-2s will be required to be submitted to Social Security and Forms 1099-MISC will be required to be submitted to the IRS with the same due date as to the recipient. This accelerated timeframe should pose a significant hindrance for those who submit fraudulent returns. However, there is still the issue that the IRS will start processing tax returns during the month of January, usually on or about January 20, leaving a window for fraudulent tax returns to be submitted and processed before the IRS has the opportunity to match data.

The IRS has estimated that it averages approximately one million breach attempts daily. However large that number might be, as a taxpayer I would expect that every attempt would be defeated. Unfortunately, over the past year, the IRS has had actual system breaches. First, the IRS online transcript program, "Get Transcript", was compromised in May 2015 and the number of accounts that the IRS admitted were affected has doubled several times. In February 2016 the IRS announced the affected accounts exceeded 700,000. The second breech that occurred recently related to the Identity Protection PIN (IP PIN) retrieval tool that is contained on the IRS website and is more troubling than the prior breach. The taxpayers who have IP PINs have already been victims of tax refund fraud and obtained the six digit IP PIN to prevent further un-

authorized access or filings. This tool had been using the same interface as Get Transcript but had remained available to the public and, unfortunately, those less scrupulous. Finally, the IRS took this page offline in February 2016, nearly nine months after the initial Get Transcript breach.

The March 2016 GAO report identified that the IRS has improved access controls, but noted that weaknesses still remain. One of the primary concerns addressed by the GAO surrounds the authentication of the user ID. The IRS has employed a multifactor approach using two or more factors to achieve authentication. This provides the basis for establishing accountability and for controlling access to the system. Their systems require that Homeland Security Presidential Directive 12-Compliant Authentication be implemented for IRS local and network access accounts. This involves password-based authentication with passwords that are not found in dictionaries and expire at a maximum of 90 days. This same protocol should be implemented for all user accounts, including e-services.

The direct deposit of refunds is a fast, inexpensive and relatively secure means of issuing refunds. The IRS utilizes banking's ACH system, whereby a refund goes to a selected financial institution based upon their respective routing or ABA number. If an account number exists within the institution, the refund goes into the account. The IRS is mandated to process refunds within 21 days, unless additional processing time is required. Prior to the current Modernized e-File (MeF) system, the IRS had been operating on a "accept by Thursday, refund following Friday" schedule. Often under the MeF system, refunds have been processed even quicker. Taxpayers have grown accustomed to getting the quick refund and now wonder if there is a problem when it is taking longer than a week for their refund to appear in their account.

Social Security Administration uses a banking "pre-note" to verify the accuracy of the recipient's banking information prior to the initial payment. The financial institution has five days to verify the information and notify SSA if there are errors or discrepancies. Failure to notify SSA could result in the institution being held liable for the funds if the funds are misdirected. Unfortunately, the IRS refund system does not include pre-note account verification. Funds are simply transmitted through the ACH network to the respective institution. Once deposited, there is no control on the usage of funds and often where there is fraud those deposits are moved immediately upon receipt. The implementation of a pre-note system could result in a significant reduction of the annual $3.1 billion misappropriation of government funds.

As discussed, Congress has mandated 21 days for refunds to be processed. While it is easy to understand that taxpayers want their refunds processed as quickly as possible, one must ask a simple question. Is paying a tax refund in seven to ten days a prudent use of taxpayer dollars? A recent survey by Princeton Research Associates noted that 22% of taxpayers surveyed would wait up to six to eight weeks for their refunds if they knew it would combat identity theft. **NCCPAP** members feel that simply using the pre-note tech-

nology that already exists and is used throughout the financial industry would allow taxpayers to receive their refunds promptly while reducing fraud.

Unfortunately, despite all of the efforts of the IRS and Congress to curb ID theft, often the cause is unscrupulous preparers that are often unregulated by any authority. **NCCPAP** urges Congress to pass legislation to provide the IRS the necessary authority to regulate all tax preparers and required paid preparer to meet minimum standards. Currently, only CPAs, EAs and attorneys are subject to the requirements of IRS Circular 230.

In conclusion, ID theft is an issue that initially gained traction with Congress in 2012. Much has occurred since the initial hearings and, unfortunately, the criminals have taken more steps to obtain information than the IRS has been able to block. The IRS is not alone in this battle. It seems that not a week goes by where there is not news of a major corporation announcing that their systems had been hacked. Taxpayers have become victims of ID theft through these breaches and do not necessarily understand the importance of contacting the IRS. While knowing that the IRS successfully thwarts approximately one million breach attempts each day is comforting, we should keep in mind that even one successful breach could be catastrophic to not only the IRS but to the taxpayer. Often, taxpayers do not realize they have been a victim of ID theft until their electronically filed tax return gets rejected. Once a taxpayer has been victimized, they expect to obtain an IP PIN from the IRS and starting in January 2017 they will. In Florida, Georgia and Washington, DC where ID theft has been rampant, the IRS implemented a voluntary IP PIN program. Unfortunately, this program failed to achieve the number of participants to make the program successful.

Taxpayers are urged to protect their personal data, but with widespread Internet usage, online shopping and criminals waiting to pounce on unsuspecting victims, ID theft continues to grow. Individual and businesses remain targets of cyberattacks and must remain cautious when opening emails and attachments, visiting web pages and simply paying for the family groceries.

There are several electronic filing options available to taxpayers. Many taxpayers use Free File, thirteen IRS-approved free e-filing tax service sites. In a recent audit performed by the Online Trust Alliance (OTA), six of the thirteen websites failed due to poor site security and not taking steps to help protect consumers from fraudulent and malicious email.

IRS Commissioner Koskinen had the foresight to convene the initial Security Summit in 2015, which has proven to be successful. Unfortunately, the criminals always seem to be pushing the envelope further and further. Their approach is more focused and better funded. The Security Summit has now expanded its focus to include additional user groups, including tax practitioners, to further address cyber security and develop a multi-tiered approach to combat it. The only way to truly combat ID theft is to incorporate input from various sectors of the marketplace. This is a problem impacting businesses and taxpayers worldwide and will require global ef-

forts to minimize and hopefully resolve. **NCCPAP** calls on Congress to provide the necessary funding to continually monitor, modernize and upgrade IRS systems to minimize and eliminate data security breaches. The first step would be Congress reauthorizing Streamlined Critical Pay Authority to allow the IRS secure top IT talent without a three to six month waiting period.

Thank you for the opportunity to present this testimony and I welcome your questions.

Respectfully submitted,

Stephen F. Mankowski, CPA
Executive Vice President, **NCCPAP**

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
P: 703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org
National Association of Federal Credit Unions | nafcu.org

April 19, 2016

The Honorable Steve Chabot
Chairman
Small Business Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Nydia Velázquez
Ranking Member
Small Business Committee
U.S. House of Representatives
Washington, D.C. 20515

Re: Cyber and Data Security

Dear Chairman Chabot and Ranking Member Velázquez:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today regarding tomorrow's hearing entitled, "Small Business and the Federal Government: How Cyber Attacks Threaten Both." A primary concern of credit unions and their 103 million members continues to be ensuring that our nation's retailers have the data and cyber security standards to protect consumers' information. We thank you for holding this important hearing and applaud your continued leadership on this matter.

NAFCU supports many of the ongoing efforts to strengthen the existing mechanisms in place to address cyber security issues, such as the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). These organizations work closely with partners throughout the government, creating unique information sharing relationships that allow threat information to be distributed in a timely manner. NAFCU also worked with the National Institute of Standards and Technology (NIST) on the voluntary cyber security framework released in 2013, designed to help guide financial institutions of varying size and complexity in reducing cyber risks to critical infrastructure.

Still, we believe more needs to be done on the data security front. Data security is an important part of the cyber security discussion and every time a consumer uses a plastic card for payment at a register or makes online payments from their accounts, they unwittingly put themselves at risk. Traditionally, consumers have trusted that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, in the wake of several headline grabbing retailer breaches in recent years, this does not seem to be the case today.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that financial institutions, including credit unions, have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act*. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, even though they are often victimized in data breaches or by data thieves. While these entities still get paid, financial institutions bear a significant burden as

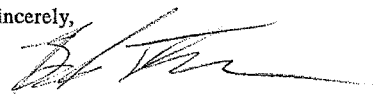
the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

The ramifications for credit unions and their members have been monumental. A February 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were $226,000 on average. Of their losses, respondents expect to recoup less than 0.5%, which amounts to less than $100 on average.

NAFCU believes legislation pending before the House, H.R. 2205, the *Data Security Act of 2015,* would help address these concerns. This legislation would create a national standard of data security for all industries that handle sensitive information based on the standards in *Gramm-Leach-Bliley Act* (GLBA), a key priority of NAFCU. It would also recognize that it is not productive to duplicate data protection and consumer notice requirements that are already in place for credit unions under GLBA. This legislation passed the House Financial Services Committee with a strong bipartisan vote last December. We urge committee members to support this legislative approach to this issue.

Thank you for your attention to this important matter. We look forward to tomorrow's hearing and working with the committee as you move forward in addressing cyber and data security issues. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Senior Associate Director of Legislative Affairs, Chad Adams, at (703) 842- 2265.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Small Business Committee

○